2012-03

Identity Verification Systems as a Critical Infrastructure

Clarkson, Robert D.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IDENTITY VERIFICATION SYSTEMS AS A CRITICAL INFRASTRUCTURE

by

Robert D. Clarkson

March 2012

Thesis Advisor:	Rodrigo Nieto-Gomez
Second Reader:	Erik Dahl

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Identity Verification Systems as a Critical Infrastructure		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Robert D. Clarkson			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Identity management systems are essential to U.S. homeland and economic security. Systemic fragility has been exploited to facilitate terrorist travel and criminal evasion. The widespread dissemination and use of fraudulent identity documents exponentially complicates efforts to target terrorists and other persons who pose a threat to homeland security. Underage drinkers and illegal immigrants are common supporters and users of the fraudulent document industry. No single source can determine the net effect that these entities have in degrading identity system utility.

Identity verification systems are large networks, susceptible to degradation, and vital to other sectors of critical infrastructure. Current attempts to analyze identity systems are segmented and fractured. Analyzing these systems as a comprehensive critical infrastructure provides a necessary framework of language and concepts that are familiar to policymakers. This thesis is focused on providing a thorough understanding of the vulnerabilities associated with weak identity systems and analyzing identity systems as a critical infrastructure.

14. SUBJECT TERMS Identity System, Identity System Fragility, Identity Theft, Identity Fraud, Terrorist Travel, Organized Crime, Critical Infrastructure, International Travel, U.S.-VISIT, Passport Fraud, Driver's License Fraud, REAL ID Act of 2005, Illegal Immigration.			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IDENTITY VERIFICATION SYSTEMS AS A CRITICAL INFRASTRUCTURE

Robert D. Clarkson
Lieutenant, United States Navy
B.A., University of West Florida, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2012

Author: Robert D. Clarkson

Approved by: Rodrigo Nieto-Gomez
Thesis Advisor

Erik Dahl
Second Reader

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Identity management systems are essential to U.S. homeland and economic security. Systemic fragility has been exploited to facilitate terrorist travel and criminal evasion. The widespread dissemination and use of fraudulent identity documents exponentially complicates efforts to target terrorists and other persons who pose a threat to homeland security. Underage drinkers and illegal immigrants are common supporters and users of the fraudulent document industry. No single source can determine the net effect that these entities have in degrading identity system utility.

Identity verification systems are large networks, susceptible to degradation, and vital to other sectors of critical infrastructure. Current attempts to analyze identity systems are segmented and fractured. Analyzing these systems as a comprehensive critical infrastructure provides a necessary framework of language and concepts that are familiar to policymakers. This thesis is focused on providing a thorough understanding of the vulnerabilities associated with weak identity systems and analyzing identity systems as a critical infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CIA	Central Intelligence Agency
COPS	Community Oriented Policing Services
DHS	Department of Homeland Security
DMV	Department of Motor Vehicles
DoD	Department of Defense
DoJ	Department of Justice
DoS	Department of State
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
GAO	Government Accountability Office
HSPD-24	Homeland Security Presidential Directive 24
HSPD-7	Homeland Security Presidential Directive 7
IAFIS	Integrated Automated Fingerprint Identification System
ID	Identification
IDENT	Automated Biometric Identification System
INS	Immigration and Naturalization Service
IRS	Internal Revenue Service
LAPD	Los Angeles Police Department
MBVA	Model-Based Vulnerability Analysis
NSPD-59	National Security Presidential Directive 59
RFID	Radio Frequency Identification
SSN	Social Security Number
TSA	Transportation Security Administration
USPS	U.S. Postal Service
U.S.-VISIT	U.S. Visitor and Immigrant Status Indicator Technology

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisor, Dr. Rodrigo Nieto-Gomez, for believing in this project and pushing it to its full potential. His enthusiasm is infectious and level of knowledge is unparalleled. Dr. Nieto-Gomez was a significant driving force behind the development of this thesis. My second reader, Dr. Erik Dahl, also applied his significant experience, expertise, and acute attention to detail to shape this project. Thank you both for your timely and relevant guidance.

As a victim of identity theft, I have been personally touched by the problems caused by fragile identity systems. My credit was threatened by fraudulently obtained credit cards and medical bills totaling nearly $30,000. My criminal record was stained when someone with a fraudulent driver's license (my information, his picture) received a DUI charge, failed to appear in court, and caused a warrant to be issued for my arrest. Additionally, I received a steady stream of traffic citations from the State of New York that required me to submit notarized affidavits to counter every citation. I have spent hundreds of hours making phone calls, writing letters, and trying to convince numerous people that someone other than myself used my information to commit these offenses.

Throughout my turbulent journey, there have been very few people who have listened to my story and taken the time to truly help. In late 2010, I was introduced to Mr. Rich Stone, the Deputy Escambia County Tax Collector in my home state of Florida. Mr. Stone listened to my story and informed me of a process that would change my driver's license and substantially alleviate the stream of frauds committed against me. Mr. Stone relayed my story to the Escambia County Tax Collector, Ms. Janet Holley, and together they fought through multiple levels of bureaucracy on my behalf. I received my new license because of their actions and can report that I have not been victimized since. I would like to offer my most sincere thanks to Mr. Rich Stone and Ms. Janet Holley for taking a personal interest in my case, zealously representing my interests, and acting above and beyond all expectations.

Finally, this thesis project would not have materialized without the love and support of my family. I would like to thank my wife, Macey, for her patience and understanding. She graciously shouldered my half of family responsibilities throughout this process. And special thanks to my 6-month-old son, Cohen, for motivating and inspiring me to be a better person every day.

I. INTRODUCTION

A. MAJOR RESEARCH QUESTIONS

Identity theft and fraudulent document production are reaching alarming levels in the United States. The Federal Trade Commission (FTC) estimates place the annual cost of identity-related crimes at $50 billion.[1] Since reporting began in 2000, identity theft has dominated as the most reported crime, and the overall number of reports continues to increase each year.[2] But identity theft is only part of a greater identity problem.

Identity fraud encompasses the use of stolen identity or fictitious identity information to falsely represent oneself. In addition to numerous financial crimes, identity fraud has been used to facilitate terrorist travel and criminal evasion. Vulnerabilities in the nation's identification management systems threaten economic stability and leave a serious gap in homeland security.

In 2003, the U.S. Government Accountability Office (GAO) released a report following the investigation of identity credential issuing agencies in multiple states across the nation. Undercover investigators attempted to obtain genuine driver's licenses, enter the United States from foreign destinations, gain access to federal buildings, and purchase firearms using fraudulent documents. They were successful in every instance.[3] While most think of identity theft and document fraud as an economic crime, this thesis aims to explore the extent to which weak identification systems constitute a threat to homeland security.

Homeland Security Presidential Directive 7 (HSPD-7) defines critical infrastructure as any sector that has the potential to "impair Federal departments and agencies' ability to perform essential missions…undermine State and local government

[1] Kristin M. Finklea, "Identity Theft: Trends and Issues," Congressional Research Service, R40599 (2010), 10.

[2] Ibid.

[3] U.S. Government Accountability Office, "Counterfeit Identification and Identity Fraud Raise Security Concerns," GAO-03–1147T (Washington, D.C., May 25, 2011): 1.

capabilities to maintain order...[or] undermine the public's morale and confidence in our national economic and political institutions."[4] While identity verification systems are not a recognized sector of critical infrastructure, national economic and political institutions rely on identity to function. Taxation, government benefits, citizenship, and the legal system are all governmental functions that can be undermined by fragile identity systems.

Similarly, economic processes such as mortgages, credit lines, and banking are equally susceptible to identity fraud. Stealing identity information or misrepresenting true identity allows perpetrators to acquire goods or services without consequence. Identity theft victims are often unaware that their information has been compromised until they apply for credit and are denied. Credit institutions, eager to issue credit lines, accept the risk of fraud and pass the cost along to responsible consumers. Writing off losses is often less of an investment than persuing an investigation against suspected cases of fraud.

The basic functions of identity systems can be summarized into three categories. First, the system must *identify* and distinguish you from other users of the system.[5] Second, the system must *authenticate* your identity.[6] Current systems rely on token identifiers such as driver's licenses or passports to confirm that you are who you say you are. Finally, the system must determine your level of *authorization*.[7] Having a passport that correctly identifies you does not give you the authorization to enter every country. These basic functions must work in concert to protect the integrity of the system.

Identity verification systems are large networks, susceptible to degradation, and vital to other sectors of critical infrastructure. Consequently, should identity systems be considered a sector of critical infrastructure? Analyzing these systems as a critical

---

[4] Text of the Homeland Security Presidential Directive/HSPD-7 on the Homeland Security Digital Library website, https://www.hsdl.org/?view&doc=78291&coll=limited (accessed June 4, 2011).

[5] Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (New York: Copernicus Books, 2003), 182.

[6] Ibid., 183.

[7] Ibid.

infrastructure may provide a necessary framework that is largely absent in any existing literature. This framework includes language and concepts familiar to policymakers and scholars of network analysis.

Additionally, what are the common security implications of weaknesses in identity verifications systems? Pinpointing areas of fragility is the first step in developing a strategy to counter fraud and increase capability. This thesis will seek to analyze identity management systems as a critical infrastructure analog and will examine potential solutions from an all-hazards approach.

B. LITERATURE REVIEW

In a 2006 article on identity theft, Keith B. Anderson wrote that "The literature on identity theft, both conceptual and empirical, is in its infancy."[8] Seven years later, this description still holds true. Many authors have written on particular aspects of identity theft, but none have succeeded in completing a singular comprehensive and informative piece of quintessential literature. Instead, the literature addressing identity theft and document fraud is limited to specific areas of interest and takes many different approaches. While the vast majority of existing work focuses on economic consequences of weak identity systems, few articles describe the threat to homeland security. This review will examine major works of existing literature that address identity system fragility and will highlight areas for additional research.

Personal information can be compromised in a number of ways. The most common means of information loss, as reported by the Federal Trade Commission (FTC), are careless disposal of sensitive information in the trash, mail theft, hacking of business records, employees abusing access to business databases, elaborate fraudulent credit card scanners, stolen purse or wallet, or phone and Internet scams.[9] The FTC also reports that identity thieves steal information in order to commit credit card fraud, establish utilities,

---

[8] Keith B. Anderson, "Who are the victims of identity theft? The effect of demographics," *Journal of Public Policy & Marketing*, 25, no. 2 (2006): 160.

[9] Federal Trade Commission, "Take Charge: Fighting Back Against Identity Theft," February 2006, on the Federal Trade Commission website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.

counterfeit financial documents, file for bankruptcy, make large purchases, obtain identity documents or employment, and evade law enforcement.[10] Many consumers are aware of these threats and take limited precautions to protect against them.

Consumers typically provide characteristics such as date of birth, social security number, and mother's maiden name in order to verify who they are. But defining the unique characteristics that distinguish an individual from among others is "among the most elusive and difficult concepts confronting scholars and researchers."[11] Identification requires a comparison and authentication of presented characteristics against known metrics. However, many of the current metrics are easily spoofed or reproduced.

There are three basic identity verification methods that are widely accepted among experts in the field. "Knowledge based" identity requires a consumer to produce information unique to that person.[12] "Token-based" identity is based on an identification document, like a driver's license or passport.[13] "Biometric" identity uses unique physical characteristics to differentiate individuals.[14]

Newer and more controversial methods of proving identity are radio frequency identification (RFID) chips or location tracking through mobile telephone service providers.[15] While all of these methods provide some level of security, each is susceptible to unauthorized reproduction. LoPucki explains that "creditors and credit-reporting agencies often lack both the means and the incentive to correctly identify the persons who seek credit from them or on whom they report."[16]

---

10 Ibid.

11 Charles D. Raab, "Social and Political Dimensions of Identity," in *IFIP International Federation for Information Processing*, ed. Fischer-Hubner (Boston: Springer, 2008): 4.

12 Roger Clarke, "Human Identification in Information Systems: Management Challenge and Public Policy Issues," *Information Technology & People*, 7, no. 4 (1994): 14.

13 Ibid.

14 Ibid., 19.

15 Ruth Halperin and James Backhouse, "A Roadmap for Research on Identity in the Information Society," *Identity Journal Limited*, 1, no. 1 (2008): 75.

16 Lynn LoPucki, "Human Identification Theory and the Identity Theft Problem," *Texas Law Review*, no. 01-1 (2001): 94.

The White House addressed the threat to identity systems in its National Strategy for Trusted Identities in Cyberspace. The strategy outlines a technology-driven solution to restore consumer confidence in Internet purchasing.[17] The Identity Ecosystem "is an online environment where individuals and organizations can trust each other because they follow agreed-upon standards and processes to identify and authenticate their digital identities—and the digital identities of organizations and devices."[18] The strategy provides a fictitious example describing how the system might work to request medical records using the Identity Ecosystem:

> Keisha uses the browser on her cell phone to access the hospital website. The browser authenticates the hospital's website domain so that Keisha knows she is not sending information to a fraudulent site. Keisha has a digital certificate issued by her trustmarked cell phone carrier (also her IDP), and the hospital validates the authenticity of the credential, her cell phone, and her digital identity.[19]

While the Identify Ecosystem is supposed to provide a safe environment between accredited consumers and providers, the strategy does not explore the possibility of Keisha's cell phone being stolen or otherwise compromised. Additionally, it does not consider the role of hackers in corrupting the information systems that the Identity Ecosystem relies upon. The strategy outlines an initial approach, but is absent of contingencies and specifics.

The Government Accountability Office (GAO) released a statement by its director of strategic issues to the Senate Subcommittee on Fiscal Responsibility and Economic Growth regarding initiatives to assist victims of tax fraud. In particular, the director addressed employment and refund fraud.[20] He praised the IRS for taking steps to resolve, detect, and prevent identity theft in its tax returns, but was critical of confidentiality laws

---

17 Howard A. Schmidt, "National Strategy for Trusted Identities in Cyberspace," April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (accessed June 6, 2011).

18 Ibid.

19 Ibid.

20 GAO, "Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers," GAO-11–674T (Washington, D.C., May 25, 2011): 1.

that prevented the IRS from coordinating with other agencies or taxpayers to catch perpetrators.[21] Bureaucratic limitations constrain efforts to investigate or track imposters.

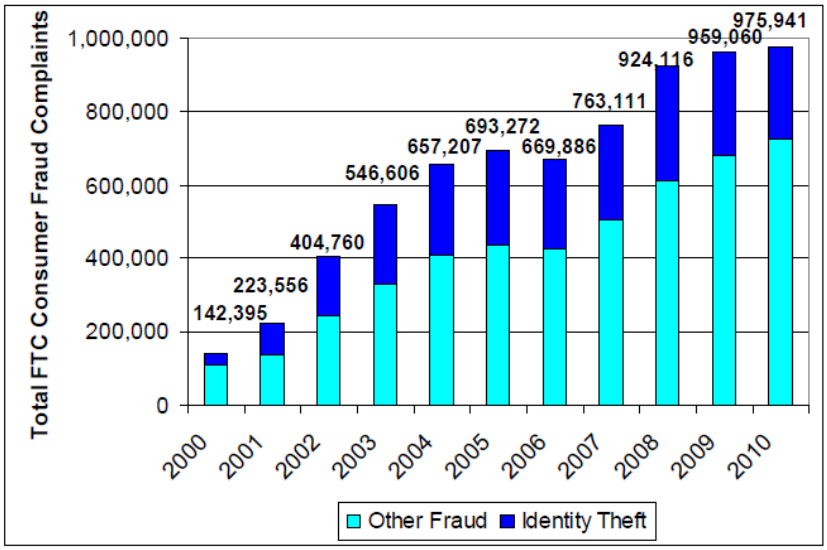

Figure 1. Total FTC Consumer Fraud Complaints[22]

Economic crimes resulting from identity theft represent the majority of FTC complaints (Figure 1), but these crimes tend to be relatively small in scale. Criminal record identity theft, on the other hand, represents a very real threat to homeland security. Despite this risk, the FTC consumer guide mentions misuse of identification for criminal evasion in one section of the 52-page document. Criminal record identity theft is a tactic that has been used by illegal immigrants, criminal organizations, and terrorists.[23] This tactic allows an imposter to launder his own identity and insulate himself from detection by law enforcement and operate with near impunity.

---

21 Ibid.

22 Kristin M. Finklea, "Identity Theft: Trends and Issues," Congressional Research Service, R40599 (2012), 10.

23 Pearl, "It's Not Always about the Money: Why the State Identity Theft Laws Fails to Adequately Address Criminal Record Identity Theft," 179.

Organized crime plays a broad and pervasive role in the undermining of identity verification systems. In general, identity crimes require a network.[24] Organized transnational criminal networks are optimized for collecting stolen identity, converting it to a useable form, and disseminating it for sale. Jurisdictional limitations and the lack of international cooperation greatly contribute to the success and sustainment of these organizations. Attempts to dismantle organized crime are largely ineffective without comprehensive examination of the entire organization. Network analysis is essential to obtain a larger perspective and identify critical nodes of network structure and operation.

Ted G. Lewis defines a network as "a collection of nodes and links that connect pairs of nodes."[25] His framework is described in terms of physical infrastructure protection. Lewis explains that "Network theory is powerful because of its generality and our ability to apply known analysis techniques to the network model."[26] In essence, networks can be described using mathematical probabilities that identity critical nodes. This knowledge could potentially be used by policymakers to protect against attack on the homeland or develop strategies to dismantle target networks.

Social network analysis allows network analysis principles to be applied to criminal and terrorist organizations. Once a social network is mapped, "this knowledge can then be used to identify key individuals, relationships, and organizational practices."[27] Researchers have recognized the utility of social network analysis to detect fraud in specific cases, such as Internet auction fraud,[28] but have failed to examine the

---

24 Judith M. Collins, *Investigating Identity Theft: A Guide for Businesses, Law Enforcement, and Victims* (Hoboken, NJ: John Wiley & Sons, Inc., 2006), 18.

25 Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: John Wiley & Sons, 2006), 78.

26 Ibid., 79.

27 J. Todd Hamill, Richard F. Deckro, James W. Chrissis, and Robert F. Mills, "Analysis of Layers Social Networks," *IO Sphere* (2008): 2, http://www.au.af.mil/info-ops/iosphere/08winter/iosphere_win08_hamill.pdf (accessed November 17, 2011).

28 Chaochang Chiu, Yungchang Ku, Ting Lie, and Yuchi Chen, "Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches," *International Journal of Electronic Commerce* 15, no. 3, (2011): 123.

underlying problem with identity verification systems. Network analysis and critical infrastructure terminology are a start to developing comprehensive understanding of the identity meta-sector.

Government agency strategies provide vital insight as to how each agency views identity problems and what they are doing to combat them. They define the culture and specific niche of a particular agency while outlining strategic issues to be addressed. Identity theft and fraud are frequently addressed but rarely in any meaningful manner.

The 2010 Quadrennial Homeland Security Review Report and the U.S. Department of Justice Strategic Plan address identity theft as a cyber threat, but both fail to describe identity theft as a threat to homeland security.[29] The U.S. Immigration and Customs Enforcement Strategic Plan, on the other hand, highlights identity fraud as a terrorist tactic used to enter the United States.[30] Unlike the Department of Homeland Security and Department of Justice, prevention of identity fraud is included in ICE's objectives.

The Office of Community Oriented Policing Services (COPS), a liaison office within the Department of Justice, released "A National Strategy to Combat Identity Theft" in May 2006. Of all the national strategies, this document is the most comprehensive and informative. Most significantly, the strategy states:

> One of the most challenging aspects of identity theft is its potential relationship to international terrorism. Identity theft could be used broadly by crime rings that may include international members; therefore, whenever transnational crime is discussed authorities should look for a connection to terrorism. Identity theft demands the most effective police response possible.[31]

The potential link between terrorism and organized crime has received increasing attention in recent years. Some researchers have drawn similarities between the

---

[29] Department of Homeland Security, "Quadrennial Homeland Security Review Report," (2010): 56; U.S Department of Justice, "Strategic Plan: Stewards of the American Dream," (2007): 4.

[30] U.S. Immigration and Customs Enforcement, "ICE Strategic Plan: Fiscal Years 2010–2014," (2010): 3.

[31] Office of Community Oriented Policing Services, "A National Strategy to Combat Identity Theft," U.S. Department of Justice (2006): 1.

operational and organizations structures of each group.[32] Others point to organized crime as a source of revenue for terrorist organizations.[33] Both groups use stolen and fraudulent identity to sustain operations and this link demands additional research. Securing identity systems may prove to limit the scope of terrorist and criminal operations.

In 2004, the Economic Crime Institute at Utica College joined with Lexis Nexis to study the net effect of identity fraud on global and U.S. national security.[34] The resulting article outlined the size and scope of identity issues, described many of the second order effects, and provided strategic recommendations for managing fraud.[35] Although the article was extensive, it failed to present a framework for objectively analyzing the many core and satellite issues extending from identity theft and fraud. Presenting identity verification systems as a sector of critical infrastructure provides this much needed framework.

C. IMPORTANCE OF RESEARCH

The problem of identity is one that is often overlooked. Identity is necessary for commerce and governments to function but identification is not a simple process. Historically, identity was a method of social distinction rather than economic function.[36] Communities recognized individuals based on appearance, voice, first-hand knowledge, and name.[37] Developing economic systems changed the scale of identity systems from community to regional. The increase in scale of economic transactions acted to increase

---

[32] Frank S. Perri and Richard G. Brody, "The Dark Triad: Organized Crime, Terror and Fraud," *Journal of Money Laundering Control* 14, no.1 (2011): 44.

[33] Tamara Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Crime and Terrorism," *Global Crime* 6, no. 1 (2004): 129.

[34] G. R. Gordon, N. A. Willox, D. J. Rebovich, T. M. Regan, and J. B. Gordon, "Identity Fraud: A Critical National and Global Threat," *Journal of Economic Crime Management* 2, (2004).

[35] Ibid., 2.

[36] Roger Clarke, "Human Identification in Information Systems: Management Challenge and Public Policy Issues," *Information Technology & People*, 7, no. 4 (1994): 8.

[37] Ibid.

the need for a reliable system to identify persons from separate communities who may have never met.[38] Surnames and assigned account numbers helped to fulfill this need for a time.[39]

Modern transportation and communication systems have increased the scale of travel and economic transactions to a global level. Face-to-face recognition is virtually obsolete as a primary means of identification for most operations. Instead, knowledge and token-based identifiers are the most widely used identity authentication methods. Typical "knowledge-based" identifiers include name, address, phone number, mother's maiden name, and social security number.[40] Using this information, governments and business issue "token" identifiers such as birth certificates, credit cards, driver's licenses, and passports.[41]

Knowledge and token-based identifiers codify characteristics of human identity, but neither method is capable of definitively identifying one individual from another.[42] Token identifiers are usually verified using knowledge-based identifiers or checked against existing databases to increase resiliency of the system. This verification process cannot account for the duplication or misrepresentation of names, similar physical characteristics, and fraudulent tokens. Additionally, verification databases must be made widely available to be viable. This wide dissemination provides opportunities for thieves to steal knowledge-based information that is not easily changed once compromised.[43]

Biological characteristics offer an alternative to knowledge and token-based verification. Fingerprints, retinal scans, facial recognition software, and DNA provide technically and economically feasible options to governments and businesses.[44] In the United States, however, fears of government abuse of power make these options socially

---

[38] Ibid.

[39] Ibid., 13

[40] Ibid., 14.

[41] Ibid.

[42] Ibid., 17.

[43] Lynn LoPucki, "Human Identification Theory and the Identity Theft Problem," *Texas Law Review* 95, no. 1 (2001), 109.

[44] Roger Clarke, "Human Identification in Information Systems: Management Challenge and Public Policy Issues," 20.

unacceptable and contrary to national values. Providing a blood sample for a social security card or credit line is considered an "unwarranted invasion of privacy."[45] On the other hand, Europeans are generally more willing to submit to more invasive identification techniques.[46] Identity systems contain a social component that may vary from location to location making it "necessary to balance the interest of individuals in the various aspects of civil liberty."[47]

The identity system functions when all actors play by the rules of the system. However, significant security lapses can occur when thieves steal personal information and counterfeit token identifiers. Once obtained, personal information can be exploited in a number of ways. Most common is credit fraud, whereby an imposter receives a credit line and purchases goods or services. Although costly, this form of identity theft is containable. A victim has the power to cancel the fraudulent account and dispute the charges.

Identity document fraud represents a more difficult and dangerous problem.[48] Fraudulent documents can be manufactured or genuine documents can be altered. When a valid identity is used to manufacture a fraudulent document, the imposter has a greater chance of operating undetected. For example, an imposter who is stopped for a traffic violation can present a driver's license with his picture and someone else's identity information. When the identity is checked against law enforcement databases, the imposter's criminal history is protected from discovery while his victim receives the traffic citation.

Federal law prohibits knowingly possessing, transferring, or using any fraudulent identity document.[49] However, a thriving clandestine document industry eagerly supplies high quality forgeries in response to demand. Teenagers, illegal immigrants, and other

---

[45] LoPucki, "Human Identification Theory and the Identity Theft Problem," 111.

[46] Clarke, "Human Identification in Information Systems: Management Challenge and Public Policy Issues," 27.

[47] Ibid., 30.

[48] G. R. Gordon, N. A. Willox, D. J. Rebovich, T. M. Regan, and J. B. Gordon, "Identity Fraud: A Critical National and Global Threat," *Journal of Economic Crime Management* 2, (2004): 3.

[49] 18 U.S.C. § 1028 (a)(1–4).

customers can access this service with no more effort than an Internet search. Websites traced to China take personal information and payment online, and then ship fraudulent driver's licenses that are "indistinguishable" from their authentic counterparts.[50] In addition to facing criminal charges, users of this service may be victimized by the overseas criminal organizations that manufacture their fraudulent licenses.[51] More disturbing than underage drinking or illegal immigration is the very real possibility that terrorists will acquire and use these high-quality documents in the course of an operation in the United States.

The 9/11 Commission Report recognized that, "For terrorists, travel documents are as important as a weapon. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack."[52] Current identification systems are fragile and easily susceptible to manipulation. In the past, this weakness allowed terrorists to move unfettered and participate in criminal activity to finance their operations.[53] While stricter measures are being implemented, gaps in homeland security still exist.

In the summer of 2011, Olajide Oluwaseun Noib successfully boarded a flight to New York from Los Angeles using an expired boarding pass and a student identification card. The 24-year-old with dual U.S.-Nigerian citizenship presented his student ID and a police report to support his story that his passport had been stolen. Noib was not identified until his flight was underway and airline personnel realized he was sitting in a seat that was supposed to be vacant.[54]

---

[50] Jim Avila, "Risky Business: Teens Buying Fake IDs From Overseas Via Internet," *ABC News*, August 5, 2011, accessed August 15, 2011, http://abcnews.go.com/U.S./ParentingWeek/risky-business-teens-buying-fake-ids-overseas-Internet/story?id=14243205#.TkVKVfdgn4M.e-mail.

[51] Nancy Harty, "Fake IDs Made in China Seized; Underage Kids Cited," *CBS News*, July 22, 2011, accessed August 15, 2011, http://chicago.cbslocal.com/2011/07/22/fake-ids-made-in-china-seized-underage-kids-cited/#.TkVH-8IFfV4.e-mail.

[52] National Commission on Terrorist Attacks upon the United States, Thomas H. Kean, and Lee Hamilton. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. (Washington, D.C.: National Commission on Terrorist Attacks upon the United States, 2004), 384.

[53] Gordon et al., "Identity Fraud: A Critical National and Global Threat," 13.

[54] Carly Schwartz, "Olajide Oluwaseum Noibi Sentenced to Time Served in LA Stowaway Case," *Huffington Post*, November 28, 2011, http://www.huffingtonpost.com/2011/11/28/olajide-oluwaseun-noibi-stowaway_n_1117716.html (accessed January 16, 2012).

Identity is a valuable resource that various sectors of infrastructure rely upon to function. Vulnerability analysis is needed to create strategies for enhancing identity verification systems used by government and commerce. Solutions must be comprehensive and viable to be effective. Network analysis tools used for infrastructure and social research offer significant advantages over current investigative methods and represent an all-hazards approach.

If documents cannot distinguish person from person, then what can? What are the characteristics that define human identity? How can these characteristics be harnessed to create stronger economic, immigration and criminal management systems? Answering these questions is essential to address weaknesses in current identity systems. While this thesis does not contain all the answers, it aims to further understanding of the problems associated with identity systems and spur further research into the subject.

D. ORGANIZATION AND METHODOLOGY

The goal of this research is to provide a thorough understanding of the vulnerabilities associated with weak identity systems and analyze weaknesses in terms of critical infrastructure. Previous and existing vulnerabilities will be described using case studies. Some of these examples will be supplemented with personal experiences of the author in dealing with the consequences of identity theft. Current policy will be analyzed for effectiveness and sufficiency in protecting identity management systems from existing threats to homeland security.

Chapter II will examine identity from the terrorist perspective and review case studies to pinpoint how identity has been exploited in the past. Chapter III will discuss how organized crime supplies a thriving fraudulent identity document industry while Chapter IV will explore other common users of fraudulent documents who contribute to the undermining of the identity verification system. Finally, Chapter V will analyze the preceding evidence in terms of critical infrastructure while providing recommendations from an all-hazards approach.

THIS PAGE INTENTIONALLY LEFT BLANK

II. TERRORIST EXPLOITATION OF IDENTITY SYSTEMS

A. INTRODUCTION

Identity management is an essential function of terrorist operations. *The 9/11 Commission Report* recognized that "for terrorists, travel documents are as important as a weapon. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack."[55] Consequently, fragility within identity systems represents a risk to global and U.S. homeland security.

Document alteration and fabrication are favored terrorist tactics since many nations have failed to create comprehensive systems capable of checking documents against databases and other unique identifiers. Given the interconnectedness of the international travel system, a weakness in one region constitutes a weakness for the entire system. Ramzi Yousef and Ahmed Ressam are two al-Qaeda operatives who applied common terrorist tactics and techniques subvert international security measures.

The 9/11 hijackers successfully entered the United States, obtained state driver's licenses, and avoided detection by exploiting the limitations of numerous identity systems. Since that time, the Department of Homeland Security has overseen multiple programs designed to prevent operatives from entering the United States or obtaining identity documents. Many of these programs have not been completely implemented or are still susceptible to fraud. This chapter will analyze examples of terrorist evasion and identity acquisition tactics, followed by an evaluation of efforts to counter these threats.

[55] National Commission on Terrorist Attacks upon the United States, Thomas H. Kean, and Lee Hamilton. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (2004), 384.

B. THE INTERNATIONAL TRAVEL SYSTEM

In 2010, the United Stated received nearly 60 million international travelers.[56] The overwhelming majority of these travelers came as tourists or to conduct business. The challenge for the U.S. Department of Homeland Security (DHS) and its constituent agencies is to distinguish known and potential terrorists from the legitimate travelers.

International travel represents a significant sector of the American economy. In additional to supporting 1.1 million domestic jobs, international tourists represent 7% of all U.S. exports.[57] Actions taken to detect terrorists often slow international travel procedures, are cumbersome, and deter potential travelers. But the risk to U.S. homeland security, as demonstrated by 9/11, requires an identification process that is user friendly and effective at detecting terrorists.

Prior to traveling to the United States, foreign nationals must apply for a visa. Immigrant visas are issued to persons wishing to remain in the United States for an extended period of time. Nonimmigrant visas are for visitors planning a temporary stay. Foreigners traveling from one of the 36 countries participating in the Visa Waiver Program are not required to apply for a visa unless planning to stay in the United States for more than 90 days.[58]

Visa applications and passports are submitted for review at U.S. consulates overseas. The Department of State processes visa requests and determines eligibility to travel to the United States. If approved, the applicant may proceed to a U.S. port of entry. Immigration officers then review all applicable identity documents and grant final authorization to enter the United States.[59]

---

[56] Office of Travel and Tourism Industries, "International Visitation to the United States: A Statistical Summary of U.S. Visitation," U.S. Department of Commerce (2010), http://tinet.ita.doc.gov/outreachpages/download_data_table/2010_Visitation_Report.pdf.

[57] Ibid.

[58] Staff Report of the National Commission on Terrorist Attacks Upon the United States, Thomas R. Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States* (Franklin: Hillsboro Press, 2004): 72.

[59] Ibid., 71.

The Arrival/Departure Record, known as a Form I-94, is a system used to track visa overstays. This paper based system has two components. The arrival section requires travelers to provide basic information to include name, date of birth, nationality, sex, passport number, flight itinerary, and an address where they can be located while in the United States.[60] When the visit is complete and the traveler exits the country, the transportation carrier is required to complete and submit the departure section of the I-94 to DHS.[61]

In order to more efficiently track visa overstays and reinforce border security, Congress required the former Immigration and Naturalization Service (INS) to "implement an automated entry and exit data system that would track the arrival and departure of every alien."[62] This requirement was included in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. Subsequent modifications to the requirements of the system delayed its implementation.[63]

Following the attacks of 9/11, the entry/exit program became the foundations of the U.S. Visitor and Immigrant Status Indicator Technology (U.S.-VISIT) program. U.S.-VISIT was required by National Security Presidential Directive 59 (NSPD-59)/Homeland Security Presidential Directive 24 (HSPD-24) to "coordinate the sharing of biometric and associated biographic and contextual information with other Federal agencies and foreign partners."[64] Since December 2006, biometric functionality has been used at 300 ports of entry.[65]

---

[60] Department of Homeland Security, "Filling Out Arrival-Departure Record, CBP Form I-94, for Nonimmigrant Visitors with a Visa for the U.S.," last modified July 2, 2010, http://www.cbp.gov/xp/cgov/travel/id_visa/i-94_instructions/filling_out_i94.xml.

[61] Lisa M. Seghetti and Stephen R Vina, "U.S. Visitor and Immigrant Status Indicator Technology (U.S.-VISIT) Program," Congressional Research Service, RL32234 (2005): 3.

[62] Ibid., 1.

[63] Ibid., 5.

[64] U.S. Department of Homeland Security, "Biometric Standards Requirements for U.S.-VISIT," March 15, 2010, 1, http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_biometric_standards.pdf.

[65] GAO, "Homeland Security: Key U.S.-VISIT Components at varying Stages of Completion, but Integrated and Reliable Schedule Needed," GAO-10–13 (Washington, D.C., November 2009): 7.

U.S.-VISIT provides significant advantages over previous authentication methods. Foreign visitors are required to submit two fingerprints and a digital photograph upon entry into the United States. This information is checked against and entered into a database known as the Automated Biometric Identification System (IDENT). As of 2010, IDENT contained 108 million records.[66] These records are also checked against the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint System (IAFIS) that contains 50 million additional records.[67] U.S.-VISIT's vast database is used by four agencies within DHS as well as the Department of Defense (DoD), Department of Justice (DoJ), and Department of State (DoS).[68] "As of June 2009 … more than 150,000 biometric hits in entry [resulted] in more than 8,000 people having adverse actions, such as denial of entry, taken against them."[69]

While the biometric data contained within IDENT helps identify known terrorists and visa overstays, U.S.-VISIT has a very significant flaw. DHS has been unable to comprehensively implement biometric exit capability.[70] Without this capability, U.S.-VISIT cannot determine if persons who entered the country have exited. "Cost overruns, schedule delays, and performance problems"[71] were cited as the primary factors behind this delay.

Exit capability is not the only weakness of U.S.-VISIT. U.S.-VISIT is an identity management network that is dependent upon secure token identifiers such as passports and driver's licenses. The 9/11 Staff Report stated that "Terrorists rely on forged

---

66 U.S. Department of Homeland Security, "Biometric Standards Requirements for U.S.-VISIT," (2010): 1.

67 Ibid.

68 U.S. Department of Homeland Security, "Government Agencies Using U.S.-VISIT," http://www.dhs.gov/files/programs/gc_1214422497220.shtm, last modified March 4, 2011.

69 GAO, "Homeland Security: Key U.S.-VISIT Components at varying Stages of Completion, but Integrated and Reliable Schedule Needed," 7.

70 GAO, "Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11," GAO-11–919T (Washington, D.C., September 7, 2011): 13.

71 Ibid., 1.

passports and fake visas to move around the world unimpeded and undetected."[72] Ramzi Yousef, Ahmed Ressam, and the 9/11 hijackers are probative case studies that demonstrate common terrorist fraud tactics. These tactics are still relevant in the pursuit of secure identity management systems today.

C. TERRORIST TRAVEL TACTICS

Ramzi Yousef, a co-conspirator in the 1993 World Trade Center bombing, was apprehended with an accomplice in 1992 while attempting to enter the United States with fraudulent documents. He flew in first class from Pakistan because he believed he would receive less stringent security screenings once in the United States. In addition to numerous documents to support his false identity, Yousef was found with other passports, forgery instructions, and stamps used to alter passports. He was released in the United States after he claimed political asylum and later escaped to Pakistan. Although Yousef was eventually captured, he was able to evade law enforcement for years by using altered and fake identity documents.[73]

In 1994, Ahmed Ressam used a fraudulent passport to travel to Canada and was admitted after he claimed political asylum. His asylum claim was denied after he failed to appear in court and a warrant was issued for his arrest. Despite many misdemeanor arrests, Ressam was released and remained at large. He used a fraudulent baptismal certificate to receive a genuine Canadian passport under an alias and traveled to Afghanistan to receive terrorist training. Upon returning to Canada in 1999, Ressam devised plans to detonate a bomb at Los Angeles International Airport soon after the millennium. When Ressam was trying to cross the border, U.S. Customs officials were alerted by his nervous demeanor and discovered explosives in his rental vehicle.[74]

---

[72] Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, 47.

[73] Ibid.

[74] Kean et al., National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 176–79.

Passports are essential token identifiers within the international travel system. They are designed to confirm nationality, identity, and immigration status. Consequently, passport forgery and alteration techniques are a necessary terrorist function.

The international travel system depends on accurate screening of travelers at the point of origin. Yousef subverted this measure by bribing a Pakistani official.[75] Once he was admitted into the system, he had an Iraqi passport to support his cover story. Secondary screening revealed Yousef had no visa and his passport was fraudulent. He was arrested but released into the United States after he claimed political asylum.[76]

Passport forgery has been used by criminal and terrorist elements to support operations.[77] Forgery is used to generate funding and create documents as needed. Archaic entry and exit stamps are still being used to track travel history. Terrorist cells can forge or manipulate these stamps to "conceal their terrorist activities."[78] The *9/11 and Terrorist Travel* staff report cited "removing visas and bleaching stamps"[79] as a common alteration used by al Qaeda operatives.

Rather than forging a passport, Ressam used fraudulent breeder documents to obtain a genuine Canadian passport. This tactic represents the most favorable for terrorist operatives. Genuine passports stand up to scrutiny and support an intended narrative. Had Ressam been able to control his nerves, U.S. customs officers would have had no obvious reason to refuse him entry into the country.

The 9/11 hijackers successfully navigated gaps in immigration processing to enter the U.S. and remain undetected. The *9/11 and Terrorist Travel* staff report documents

---

75 Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States,* 51.

76 Ibid.

77 Martin Rudner, "Misuse of Passports: Identity Fraud, the Propensity to Travel and International Terrorism," *Studies in Conflict & Terrorism* 31 (2008): 103.

78 Kean et al., National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* 386.

79 Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States,* 66.

multiple instances of identity verification failure prior to the terrorist attack. As many as seven hijackers submitted manipulated passports with their visa applications to enter the United States.[80] Consular officials failed to recognize the alterations. Three hijackers "had passports that contained an indicator of Islamist extremism" and two "made false statements about prior visa and travel history on their visa applications."[81] Significant failures existed at various stages of the immigration identification process.

State Department and immigration officials had little training on document fraud, counterterrorism, or existing databases and missed all indicators of nefarious intent.[82] In cases where databases were queried, the hijackers provided alternate spellings of their names. This tactic was used over 360 times to avoid detection.[83]

Two hijackers, including Mohammad Atta, remained in the United States despite expired visas.[84] No exit system was in place and therefore no method for authorities to determine if the hijackers were still in the United States.[85] Even if these hijackers had been identified as visa overstays, there was no link with law enforcement databases to flag the infraction.[86] A flagging mechanism would have expanded the network of officials who might come in contact with the hijackers and increased the chances of capture.

The United States does not have a national identification system. Instead, state driver's licenses and ID cards are commonly used to verify identification.[87] Understanding the importance of this, all but one of the 9/11 hijackers received state

---

80 Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States,* 138.

81 Ibid., 139.

82 Ibid., 137.

83 Ibid., 4.

84 Ibid., preface, x.

85 Ibid., 7.

86 Ibid.

87 Gordon et al., "Identity Fraud: A Critical National and Global Threat," 18.

identification cards.[88] Six hijackers used their ID cards "to check in for their flights on September 11."[89] Three of the ID cards used were obtained fraudulently.[90] State identity issuing standards were much too low given the many significant uses of an identity card in the United States.

These three examples demonstrate many of the common tactics used by terrorists to subvert identity procedures within the immigration and international travel systems. Passports could also have been stolen, borrowed, rented or purchased.[91] After gaining access to the United States, these terrorists evaded capture by requesting political asylum, overstaying visas, and manipulating travel documents to conceal international travel.[92] The consistent modus operandi demonstrated that "terrorist operatives employed certain repetitive travel practices that were ripe for disruption."[93]

The Central Intelligence Agency (CIA) first outlined these types of tactics in an annual document known as the "Redbook."[94] This information was not widely disseminated even though a serious threat to homeland security was clearly recognized. The Redbook was last published in 1992 and research on terrorist travel tactics waned until after the attacks on 9/11.[95]

Many procedures and systems have been updated to narrow many of these gaps in homeland security, but significant gaps still exist. More robust training, procedures, systems and tamper-resistant documents are needed. International travel, identity, and immigration systems require seamless integration to thwart another 9/11-style attack. A recent example demonstrates this need.

---

88 Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, (2004), preface, x.

89 Ibid.

90 Ibid.

91 Rudner, "Misuse of Passports: Identity Fraud, the Propensity to Travel and International Terrorism," 103.

92 Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, (2004), 59.

93 Ibid, 65.

94 Ibid., 47.

95 Ibid., 48.

The Government Accountability Office (GAO) conducted an undercover investigation from July to December 2008 to determine if counterfeit or fraudulent documents could be used to obtain a genuine U.S. passport.[96] In four separate instances, an investigator presented various combinations of fraudulent driver's licenses, birth certificates, and Social Security Numbers (SSN) with a passport application to employees of the Department of State (DoS) and U.S. Postal Service (USPS).[97] In every instance, he was issued a genuine U.S. passport.[98]

First-time passport applications are required to be completed in person at USPS or DoS offices. The applicant's identity is checked against two forms of photo ID and copies of all documents are sent to DoS for verification. If all documentation is correct and the applicant is eligible, DoS issues a passport.

The GAO investigator used fraudulent documents of an unspecified quality to test the application process (Figure 3). At one office, he presented a counterfeit driver's license, a counterfeit birth certificate, and a SSN for a 5-year-old child.[99] The USPS accepted his counterfeit documents and DoS failed to catch the age discrepancy even though the application recorded his true age of 53.[100] At another office, the investigator used the SSN of a person who died in 1965.[101] USPS accepted the counterfeit identity documents and DoS again failed to properly verify the SSN. The investigator used one of his fraudulently obtained passports to "get a boarding pass, and pass through the security checkpoint at a major metropolitan-area airport."[102]

When the results of the investigation were released, DoS "agreed that [GAO's] findings expose a major vulnerability in State's passport issuance process."[103] DoS complained

96 GAO, "Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process," GAO-09–447 (Washington, D.C., March 2009): 3.

97 Ibid., 4.

98 Ibid.

99 Ibid., 8.

100 Ibid.

101 Ibid.

102 Ibid., 5.

103 Ibid., 9.

that it "does not have the ability to conduct real-time verification of the authenticity of birth certificates" and that they "had difficulties with verifying the authenticity of driver's licenses."[104] USPS did not issue a response.[105]

Table 1: Counterfeit or Fraudulently Obtained Documents Used to Obtain Genuine U.S. Passports

Test number	Month of application	Documents submitted as part of passport application process	Number of days between application and issuance
1	July 2008	• Counterfeit West Virginia driver's license • Counterfeit New York birth certificate • Passport application form	8 days
2	August 2008	• Genuine District of Columbia identification card obtained with fraudulent documentation • Counterfeit New York birth certificate • Passport application form	Same day (passport issued the date of application)
3	October 2008	• Counterfeit West Virginia driver's license • Counterfeit New York birth certificate • Passport application form containing SSN of a fictitious 5-year-old child, which we obtained on a previous investigation	7 days
4	December 2008	• Counterfeit Florida driver's license • Counterfeit New York birth certificate • Passport application form containing SSN of a deceased individual	4 days

Source: GAO.

Note: In all four tests, our investigator also submitted two color photographs and a passport application fee. For the second test, the investigator also submitted an e-ticket for an August 2008 flight to Germany.

Figure 2. Documents Used to Obtain Genuine U.S. Passports[106]

D. CURRENT POLICIES AND THE WAY AHEAD

Following the attacks on 9/11, significant reforms began to change the security landscape. Automated exit/entry systems, machine-readable travel documents, electronic passenger manifests, biometric requirements, and standardized technology sharing standards promised to secure Americas borders from transnational terrorism. In 2002, the Department of Homeland Security was formed to oversee the numerous government agencies responsible for implementing and utilizing these systems.

U.S.-VISIT was intended to automate the entry and exit process for foreign travelers. Biometric fingerprint scanners and passport scanners allow identity

[104] Ibid., 9.

[105] Ibid., 10.

[106] Ibid., 5.

information to be stored and checked against the IDENT and IAFIS databases. This allows known terrorists be identified at ports of entry. However, the lack of an exit component significantly degrades system utility.[107] Immigration officials do not have access to a resource that can quickly identify visa overstays.[108] Since no biometric data is taken the time of departure, exit records cannot be accurately checked against entry records.[109]

Although biometric data is a necessary component of the international travel system, it is not infallible. A terrorist may acquire a genuine passport using a fraudulent driver's license, birth certificate, social security card, or other breeder documentation. If that terrorist has not been previously biometrically scanned, he may be granted access to the United States. A biometric record would be created, but no alerts would be raised by his alias.

The Transportation Security Administration's (TSA) Secure Flight Program requires airline passengers to provide name, date of birth, and gender when purchasing tickets. The airline submits passenger manifests to the TSA to be screened against the No Fly and Selectee lists. Boarding passes are issued if the name is not on any corresponding watch list. Passenger identity is then verified using a government issued ID at the airport as part of the security screening process.[110] However, most domestic identity documents are not electronically verified. Fraudulent, stolen, or altered IDs are easily obtained and could help a terrorist pass screening.

---

[107] GAO, "Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11," GAO-11–919T (Washington, D.C., September 7, 2011): 16.

[108] Seghetti and Vina, "U.S. Visitor and Immigrant Status Indicator Technology (U.S.-VISIT) Program," 3.

[109] Ibid., 13.

[110] U.S. Transportation Security Administration, "Secure Flight Program," last modified on March 15, 2010, http://www.tsa.gov/what_we_do/layers/secureflight/.

A recent Government Accountability Office (GAO) report examined the current state of U.S efforts to thwart terrorist travel and warned that some foreign partners pose a significant risk in four key areas. First, information is not being effectively with partners due to a lack of a comprehensive terrorist screening database, unwillingness or inability to share information between countries, and/or failure to use biometric or biographical data in the screening process.[111] Information sharing requires funding and resources not readily available to many countries. But technology standards are being developed to facilitate biometric sharing in the future.[112]

Second, fraudulent documents (passports, visas, birth certificates, ect…) are inexpensive and widely available.[113] Many are indiscernible if not checked against existing databases. Surveys showed that 73% of asylum officers found "it was moderately or very difficult to identify document fraud."[114] Scarce resources limit access to crosschecking systems. Identity management is further complicated when countries fail to report lost or stolen passports, allowing valid documents to be used fraudulently.[115]

Third, the passports of some countries do not have sufficient security features to prevent reproduction or manipulation. Saudi passports, for example, lack serial numbers that could be watch listed to detect fraud.[116] Even when updated passports are issued, previous versions are valid for up to ten years after issuance.[117]

---

111 GAO, "Combating Terrorism: Additional Steps Needed to Enhance Foreign Partner's Capacity to Prevent Terrorist Travel," GAO-11–667 (Washington, D.C., July 12, 2011): 11.

112 U.S. Department of Homeland Security, "Biometric Standards Requirements for U.S.-VISIT," (2010): 1.

113 GAO, "Combating Terrorism: Additional Steps Needed to Enhance Foreign Partner's Capacity to Prevent Terrorist Travel," GAO-11–667 (Washington, D.C., July 12, 2011): 11.

114 Ibid., 19.

115 Ibid., 11.

116 Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, (2004), 66.

117 GAO, "Combating Terrorism: Additional Steps Needed to Enhance Foreign Partner's Capacity to Prevent Terrorist Travel," GAO-11–667 (Washington, D.C., July 12, 2011): 13.

Finally, the customs personnel of many countries are subject to bribes and corruption. In such countries, valid passports with fake identities can be purchased relatively inexpensively. These documents are then added to international databases and are accepted as valid elsewhere.[118]

Many U.S. agencies are investing in programs to strengthen the capabilities of foreign partners but "the international travel system is only as secure as its weakest link."[119] The current system still has significant flaws as exemplified by the case of Olajide Oluwaseun Noib.

In the summer of 2011, Olajide Oluwaseun Noib successfully boarded a flight to New York from Los Angeles using an expired boarding pass and a student identification card. At the security checkpoint, the 24-year-old with dual U.S.-Nigerian citizenship presented his student ID and a police report to support his story that his passport was stolen. Neither the security screener nor security supervisor noticed his expired boarding pass with another person's name and allowed him to pass. Noib was not identified until his flight was underway and airline personnel realized he was sitting in a seat that was supposed to be vacant. He was eventually released and ordered to pay restitution after spending five months in jail awaiting trial.[120]

Fortunately for the passengers on his flight, Noib was not a terrorist. He was an innovative transient who discovered a convenient way of subverting TSA's security measures.[121] If a homeless man with no money can easily overcome current security measures, what could a terrorist with training and financial backing accomplish?

---

118 Ibid.

119 Ibid., 30.

120 Carly Schwartz, "Olajide Oluwaseum Noibi Sentenced to Time Served in LA Stowaway Case," *Huffington Post*, November 28, 2011, accessed January 16, 2012, http://www.huffingtonpost.com/2011/11/28/olajide-oluwaseun-noibi-stowaway_n_1117716.html.

121 Ibid.

E. CONCLUSION

The 9/11 Commission Report created a list of recommendations intended to strengthen U.S. identity verification systems in response to the inadequacy of existing systems. At the top of this list was the inclusion of biometric data in databases at U.S. ports of entry.[122] While this additional layer of security is important and necessary, it does not make identity verification foolproof. Databases are only as good as the information they contain. Biometric data can help vet out aliases and simple evasion tactics such as alternate name spellings. However, biometric data cannot prevent terrorists from acquiring fake source documents with someone else's information to obtain genuine passports.

The GAO correctly surmised that "the international travel system is only as secure as its weakest link."[123] While U.S. identification and security systems are maturing, they require additional development to reach intended potential. Some foreign partners continue to allow dangerous lapses in security measures that undermine the entire system. Antiquated paper documents and a general lack of information sharing contribute to these lapses. Even when proper document security measures are in place, corrupt customs officials are available to subvert the vetting process. Strengthening U.S and foreign partner capabilities is vital to restrain terrorist travel and protect the integrity of the international travel system.

---

[122] Kean et al., National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 38.

[123] GAO, "Combating Terrorism: Additional Steps Needed to Enhance Foreign Partner's Capacity to Prevent Terrorist Travel," 25.

III. CRIMINAL ORGANIZATIONS AND IDENTITY MANAGEMENT

A. INTRODUCTION

Identity management is critical to criminal and terrorist organizations. However, the threat of organized crime plays a much broader and more pervasive role in the undermining of identity verification systems. Stolen identity information may be used to establish fraudulent lines of credit, create fraudulent documents, or sold to other criminals for profit. Each of these actions creates fractures in identity verification systems that increase fragility and decrease reliability.

Criminal organizations have taken advantage of technology to become more decentralized and anonymous. Both criminal and terrorist organizations "operate on network structures that at times intersect, such as using smuggling and other illicit means to raise cash and then employ similar fraud schemes to move their funds."[124] Similar goals and structures between criminals and terrorists allow strategies to permeate between each set of organizations.[125]

Network analysis tools have traditionally been applied to sectors of critical infrastructure. Contemporary criminal organizations, similar to terrorist groups, operate on networked constructs. This chapter will explore the structure of contemporary criminal organizations, explore the utility of network analysis, and examine links with terrorism. Additionally, this chapter will discuss the ways criminal organizations exploit weaknesses in identity verification systems while focusing on the risks to U.S. homeland security.

---

[124] Frank S. Perri and Richard G. Brody, "The Dark Triad: Organized Crime, Terror and Fraud," *Journal of Money Laundering Control* 14, no.1 (2011): 45.

[125] Tamara Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Crime and Terrorism," *Global Crime* 6, no. 1 (2004): 129.

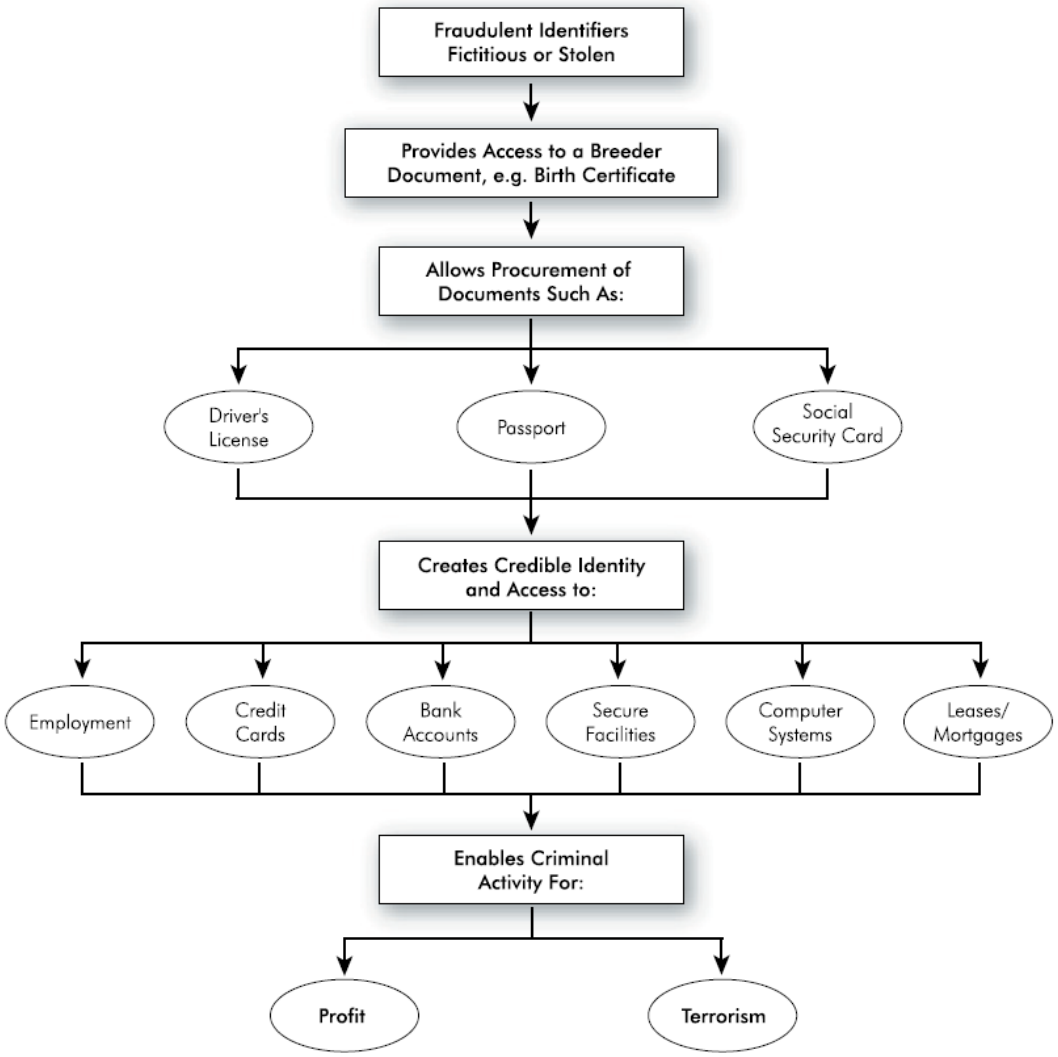

Figure 3. Uses of Fictitious or Stolen Identity[126]

B. CONTEMPORARY ORGANIZED CRIME

1. Structure

Many contemporary organized criminal enterprises adhere to a network structure rather than territorial or regional based organization. Networked organizations "are major beneficiaries of globalization…[that] take advantage of increased travel, trade, rapid money movements, telecommunications and computer links, and are well

[126] Gordon et al., "Identity Fraud: A Critical National and Global Threat," 18.

positioned for growth."[127] They are "exceptionally nimble…adapt quickly to changing political and economic realities…[and are] pragmatic and willing to forge new alliances."[128] Networked structures facilitate adaptability unlike hierarchical structures that depend on leadership and rigid, defined structure to function. Communications technologies allow decentralized nodes to collaborate across borders, often anonymously. Networking promotes collusion while protecting the identity of each respective node of the organization.

Decentralization across borders exponentially complicates law enforcement efforts to curtail crime. Jurisdictional boundaries and limits on resources restrict investigational reach. This limitation allows criminal organizations to diversify, expand, or downsize as needed with little exposure. Localized efforts to disrupt criminal operations are often ineffectual since other actors are readily available to fill any voids in the system. In this sense, it takes a network to defeat a network.[129]

Identity management is a vital function of organized crime used to camouflage criminal activity. Concealing identity protects nodes of criminal organizations from arrest or retaliation by rival organizations. Anonymity insulates the network in case any node is compromised and compelled to divulge information. That node's knowledge of the network is limited to a particular sector.

Identity crimes have been used by criminal organizations as a lucrative enterprise.[130] While these networks typically diversify into other criminal activities, identity crimes are attractive because they offer a low risk of detection while providing a

---

[127] Perri and Brody, "The Dark Triad: Organized Crime, Terror and Fraud," 45.

[128] Eric L. Olson, David A. Shirk, and Andrew Selee, "Introduction," in *Shared Responsibility: U.S. - Mexico Policy Options for Confronting Organized Crime*, ed. Eric L. Olson, David A. Shirk, and Andrew Selee (Washington, D.C.: Woodrow Wilson International Center for Scholars, 2010), accessed January 21, 2012, http://www.seguridadcondemocracia.org/administrador_de_carpetas/biblioteca_virtual/pdf/WWC_MI_Shared%20Responsibility.pdf.

[129] John Arquilla and David Ronfeldt, *Networks and Netwar: The Future of Terror, Crime, and Military* (Santa Monica, CA: RAND, 2001), 15.

[130] G. R. Gordon, N. A. Willox, D. J. Rebovich, T. M. Regan, and J. B. Gordon, "Identity Fraud: A Critical National and Global Threat," *Journal of Economic Crime Management* 2, (2004): 12.

high rate of return.[131] The Federal Trade Commission (FTC) reports that stolen identity information is most often used to commit credit card fraud, establish utilities, counterfeit financial documents, file for bankruptcy, make large purchases, gain employment or obtain identity documents.[132] Each of these tactics allow actors to sustain their criminal activity while simultaneously carrying out the responsibilities of their respective nodes of the network.

2. Network Analysis and Transnational Organized Crime

Transnational organized crime presents numerous challenges to governments and law enforcement. Jurisdictions and the lack of international cooperation greatly contribute to the success and sustainment of these organizations. Attempts to dismantle organized crime are largely ineffective without comprehensive examination of the entire organization. Network analysis is essential to obtain a larger perspective and identify critical nodes of network structure and operation.

Ted G. Lewis, a pioneer in the field of critical infrastructure, defines a network as "a collection of nodes and links that connect pairs of nodes."[133] A basic network could consist of two people talking. Each person represents a node that is linked by two-way voice communication. This network can be pictorially represented by two dots connected by a line. If the example is expanded to include ten persons having random conversations in a room, the pictorial representation becomes more complex. Inferences can be made about the relationships between each person by observing the number of interactions, the length of conversations, or physical distance maintained between nodes. This form of

131 Ibid., 8.

132 Federal Trade Commission, "Take Charge: Fighting Back Against Identity Theft," February 2006, accessed June 5, 2011, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.

133 Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: John Wiley and Sons, 2006), 78.

analysis focuses "on structural metrics rather than analysis of the characteristics of certain individual members of a group."[134] Combining this data with intelligence helps build a more concrete model for investigation.

Nodes and links are not restricted to persons or communications. They can represent "abstract concepts."[135] In the example of organized crime, a node could represent a decision maker, a critical function of operations, or location central to the organization. When basic organizational nodes are mapped, vulnerabilities can be identified and targeted.

In the field of infrastructure protection, vulnerability analysis is used to identify network weaknesses and examine the potential for failure given a particular attack. The process requires the identification of critical nodes, describing the relationship between critical nodes, and determining which nodes are essential to the sustainment of the network.[136] This process can be applied to models of transnational criminal organizations. Critical nodes of these networks can then be effectively targeted, dismantled, or fragmented according to policy objectives.

Identity crimes require a network.[137] The infrastructure of an identity theft/fraud network can be divided into three primary roles. Continuing with the critical infrastructure analogy, these roles will be referred to as generators, transmitters/ distributors, and end users.[138] Persons responsible for stealing information or blank valid documents are *generators*. They are typically closest to identity theft victims and gather

134 Chaochang Chiu, Yungchang Ku, Ting Lie, and Yuchi Chen, "Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches," *International Journal of Electronic Commerce* 15, no. 3, (2011): 126.

135 Ibid.

136 Ibid., 109.

137 Judith M. Collins, *Investigating Identity Theft: A Guide for Businesses, Law Enforcement, and Victims* (Hoboken, NJ: John Wiley and Sons, 2006), 18.

138 Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, 261.

information by retrieving it from the trash, mail theft, hacking of business records, abusing access to business databases, fraudulent credit card scanners, stealing purses or wallets, or phone and Internet scams.[139]

Once raw information or documents are acquired, generators pass it to *transmitters* or *distributors*. Transmitters are associated with larger networks and move large volumes of information to distributors. In smaller networks, transmitters and distributors can be the same actor. Distributors take identity information and convert it to a useable product for dissemination. This may be done by creating fraudulent documents or by soliciting known consumers.

Finally, the end user takes custody of the fraudulent documents or stolen information to use as needed. The end user provides the demand for identity products and sustains the criminal network. While this description of generators, transmitters/distributors, and end users is very simplistic, the particular nuances of each criminal network vary greatly. Relationships between nodes can be shaped by geographic location, level of trust, ability to communicate, and access to information. Additional actors can be subcontracted or fired in response to needs of the network. Ultimately, criminal networks grow, adapt, and respond to demand from the end user.

Network and vulnerability analysis provides investigators with a valuable resource. It creates a map of targeted organizations and identifies critical nodes of network operations. Resources can then be efficiently concentrated to accomplish policy objectives. Without network and vulnerability analysis, countering organized crime ineffectively disperses investigators across an impossibly wide front.

Hackers are persons who use knowledge and capability to hijack a system for a purpose other than it was originally intended. While this behavior is typically associated with computer networks, the concept is easily transferred to other networks as well. For instance, identity verification networks are hacked when persons misrepresent themselves as someone else. They gain access to goods and services that they would not have

[139] Federal Trade Commission, "Take Charge: Fighting Back Against Identity Theft," 2–3.

otherwise been entitled to. The following examples demonstrate some of the ways that identity systems can be hacked by criminal organizations.

3. The Criminal Element in Action

Network security is often maintained by "layering" identity crimes to complicate law enforcement efforts.[140] Judith Collins describes the creation and layering of a criminal network in her book *Investigating Identity Theft: A Guide for businesses, Law Enforcement, and Victims.*

A woman, who was hired by a temporary staffing agency, printed a list of personal information for over 3,000 employees on her last day of employment.[141] The list included "names, home, and work addresses, Social Security numbers, payroll and other personal identifying information."[142] She later sold and distributed the information to friends and family who continued using and selling it to others. Investigators eventually discovered five collaborating cells that committed a wide range of frauds for financial gain.[143]

This five-cell network remained relatively centralized and consisted of 45 individuals.[144] Members of some cells had social connections with other cells and network communication was strong. The close proximity of the primary actors allowed investigators to sift through the multiple layers of identity frauds with relative ease. The level of network complexity rises exponentially when nodes are separated by international borders, are not socially acquainted, or covered by additional layers of identity fraud as the case of Khurram Iftikhar demonstrates.

The United States Postal Inspectors were alerted by the Monterey County Sherriff's Office in 1999 that a shipment of computer components had been ordered with

---

140 Collins, *Investigating Identity Theft: A Guide for Businesses, Law Enforcement, and Victims,* 35.

141 Ibid., 21.

142 Ibid.

143 Ibid., 31.

144 Ibid., 22.

a stolen credit card number and was en route to a local parcel shipping service.[145] U.S. Postal Inspectors investigated the report and discovered many similar purchases, all sent to various branches of the shipping service within the United States. The purchaser had provided a copy of a fraudulent photo ID and forwarding addresses to overseas shipping companies.[146]

The investigation progressed slowly since U.S. investigative services could not compel foreign companies to provide additional evidence. Interviews of the victims, whose credit card information was stolen, revealed that all had attempted to purchase computer products from Internet auction sites.[147] The sites were being used to seal credit card information that would then be used to purchase computer products to be shipped to an unknown perpetrator.[148]

After three years of investigations by multiple U.S. and foreign law enforcement agencies, the fraudulently obtained shipments were eventually traced to a business in Pakistan. Khurram Iftikhar created an elaborate fraud scheme after his legitimate business had failed.[149] After obtaining credit card numbers, Iftikhar made several small purchases of computer products that were sent to the U.S. shipping service and then forwarded to overseas shipping companies. After the many smaller shipments were consolidated into larger shipments outside the United States, Iftikhar would provide shipping instructions to his company in Pakistan.[150]

Iftikhar successfully layered his criminal activity to evade detection by exploiting weaknesses in international cooperation and by using fraudulent identification. His largest failure was in streamlining the fraud process. By acting as the generator, distributor and end user, Iftikhar guaranteed that the detection of any one facet of his

---

145 Barry G. Mew, "From Pakistan to the United States: U.S. Postal Inspectors Untangle a Web of Mail Fraud, Credit Card Fraud, Internet Fraud, and Identity Theft," *United States Postal Inspection Service Bulletin* 51, no. 1 (2003): 37.

146 Ibid.

147 Ibid.

148 Ibid.

149 Ibid.

150 Ibid., 38.

operation would lead to the discovery of the entire network. Had these roles been diversified among multiple nodes, a compromised node could have been quickly replaced without degrading the efficiency of the network.

Organized crime, as it has been described above, is both an economic and homeland security threat. These fraud schemes took advantage of lapses in the security of identity management systems and international borders for personal financial gain. However, the process is replicated by untold numbers of similar organizations and individuals. The mass proliferation of stolen identity and fraudulent documents undermines the reliability of identity systems. Crime and terror organizations exploit these fractures to further their respective agendas.

C. THE "CRIME-TERROR NEXUS"[151]

Recent research suggests that criminal and terrorist organizations "have begun to reveal many operational and organizational similarities."[152] This is particularly concerning in the realm of identity verification and management. Identity manipulation is vital to the success of both organizations. "Identity fraud is a national and global threat to the security of nations and their citizens, the economy, and global commerce, as it facilitates a wide range of crimes and terrorism."[153]

The organizational line between crime and terror is becoming less well defined.[154] A decline in state-sponsorship of terror means that terrorists must turn elsewhere for funding.[155] Organized criminal activity offers a proven framework to help financially support terrorist networks. The network structure is ideal for smuggling operations, corruption, and extortion schemes traditionally seen within criminal

---

151 Perri and Brody, "The Dark Triad: Organized Crime, Terror and Fraud," 44.

152 Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Crime and Terrorism," 129.

153 Gordon et al., "Identity Fraud: A Critical National and Global Threat," 3.

154 Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Crime and Terrorism," 130.

155 John T. Picarelli and Louise I. Shelley, "Organized Crime and Terrorism," in *Terrorism Financing and State Responses*, eds. Jeanne K. Giraldo and Harold A. Trinkunas (Stanford: Stanford University Press, 2007), 39.

organizations.[156] Document fraud, in particular, provides a source of funding while simultaneously fulfilling a vital logistical need.[157] Figure 2 shows how stolen information flows through a criminal and/or terrorist network to be converted into capital or used as a logistical tool for operations.

Interactions between crime-terror nexus are evident but are not always clear.[158] Recent research on the subject provides insight as to the ways these two organizations share strategies. Established criminal organizations are primarily profit driven and are unlikely to turn entirely to terrorism since governments focus efforts against high profile, violent groups.[159]

Perri and Brody describe the crime-terror nexus as a crosspollination of tactics between criminal and terrorist groups designed to forward each other's respective agendas.[160] Terrorists may use criminal resources or tactics to support operations while criminals use terrorist methods to alter the political landscape. For example, Hassan Moussa Makki smuggled cigarettes from Indian reservations to buyers in Detroit, Michigan.[161] He trafficked "between $36,000 and $72,000 of contraband cigarettes per month between 1997 and 1999…[and] would then remit the proceeds from these illegal tobacco sales to Hezbollah."[162] Conversely, drug cartels have used targeted violence against Mexican authorities to terrorize and force officials to ignore illicit activity.[163] The sharing of tactics benefits both organizations while allowing each to focus on their core motivations.

---

156 Ibid., 43.

157 Ibid., 48.

158 Perri and Brody, "The Dark Triad: Organized Crime, Terror and Fraud," 44.

159 Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Crime and Terrorism," 133.

160 Perri and Brody, "The Dark Triad: Organized Crime, Terror and Fraud," 44.

161 Ibid., 50.

162 Ibid.

163 Ibid., 52

D. CONCLUSION

Identity management is a critical function of criminal and terrorist organizations. Weak identity systems allow criminal organizations to build networks dedicated to identity theft and fraudulent document production. These actions provide a steady source of revenue and further undermine existing identity systems. Comprehensive reforms are necessary to protect the nation from the threat to economic and homeland security.

Critical infrastructure network and vulnerability analysis provides a promising framework for identifying and dismantling criminal organizations. This process reduces "the cognitive and information overload"[164] faced by investigators and policymakers. An effective counterstrategy should involve "an integrated technological, organizational, and policy-based approach."[165] In any case, the "war on terrorism cannot be separated from the war against fraud."[166] Given the operational and organizational ties between crime and terror, a strategy to counter fraud should diminish the capacity and capability of both to function effectively.

---

164 Hsinchun Chen, "Exploring Extremism and Terrorism on the Web: The Dark Web Project," in *PAISI'07 Proceedings of the 2007 Pacific Asia conference on Intelligence and Security Infomatics*, eds. Christopher C. Yang et al. (Heidelburg: Springer-Verlag Berlin, 2007) accessed November 17, 2011, http://www.springerlink.com/content/1433543v65l61766/.

165 Ibid.

166 Perri and Brody, "The Dark Triad: Organized Crime, Terror and Fraud," 46.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COMMON VULNERABILITIES OF IDENTITY SYSTEMS

A. INTRODUCTION

The asymmetric threat of terrorism gave birth to the fields of homeland security and critical infrastructure protection. Both are relevant studies that can contribute to the security of identity verification systems. While many changes have been made to secure identity systems, terrorists still have access to quality identity information and documents. Fraudulent documents are still capable of subverting security processes. Transnational terrorism poses a real threat to homeland security, but terrorists constitute a very small percentage of the population that utilizes the international travel system.

Organized transnational crime exploits gaps in law enforcement capability and international cooperation. Identity management is a vital function of these organizations and is widely used to support operations and generate funding. The total effect of their efforts to undermine current identity systems is widely unknown since no single data source reports on the fraudulent use of identity.[167] However, the scope of system fragility can be placed into perspective by canvassing other users of fraudulent documents.

In this chapter, common sources of identity system fragility will be examined. The widespread dissemination and use of fraudulent identity documents exponentially complicates efforts to target terrorists and other persons who pose a threat to homeland security. Underage drinkers, illegal immigrants, and other criminal actors are common supporters and users of the fraudulent document industry. Strategies to counter terrorist travel and secure identity systems must take these actors into account. The cumulative impact of these actors in not known.

[167] G. R. Gordon, N. A. Willox, D. J. Rebovich, T. M. Regan, and J. B. Gordon, "Identity Fraud: A Critical National and Global Threat," *Journal of Economic Crime Management* 2, (2004): 7.

B. COMMON SOURCES OF IDENTITY FRAGILITY

1. Underage Drinkers

In the first six months of 2011, investigators in the Chicago area seized over 1700 fake driver's licenses bound for teenagers seeking access to purchase alcohol.[168] Websites traced to China took personal information and payment online, and then shipped fraudulent driver's licenses that are "indistinguishable" from their authentic counterparts.[169] The shipments arrived hidden inside inconspicuous goods at a cost of no more than $100.[170]

Users of the service face criminal charges and potential identity theft victimization. The websites require users to provide a name, photo and signature.[171] Addresses are taken from real estate websites.[172] Service providers obviously have the capability to create quality fraudulent licenses. Users who submit their real names unwittingly give the service providers a valid identity that can be sold. A consumer advocacy group warns that personal data will often "end up on a network of illegal trading sites where hackers and criminals from around the world will openly buy and sell large amounts of personal data for profit."[173]

The United States has no federal identification card and "a driver's license is used as the primary verification tool for establishing age and residency, and is the

---

168 Nancy Harty, "Fake IDs Made in China Seized; Underage Kids Cited," *CBS News*, July 22, 2011, accessed August 15, 2011, http://chicago.cbslocal.com/2011/07/22/fake-ids-made-in-china-seized-underage-kids-cited/#.TkVH-8IFfV4.e-mail.

169 Jim Avila, "Risky Business: Teens Buying Fake IDs from Overseas Via Internet," *ABC News*, August 5, 2011, accessed August 15, 2011, http://abcnews.go.com/U.S./ParentingWeek/risky-business-teens-buying-fake-ids-overseas-Internet/story?id=14243205#.TkVKVfdgn4M.e-mail.

170 Nancy Harty, "Fake IDs Made in China Seized; Underage Kids Cited," *CBS News*, July 22, 2011, accessed August 15, 2011, http://chicago.cbslocal.com/2011/07/22/fake-ids-made-in-china-seized-underage-kids-cited/#.TkVH-8IFfV4.e-mail.

171 Ibid.

172 Ibid.

173 Privacy Matters, "Computer Hacking and Identity Theft," accessed March 12, 2012, http://www.privacymatters.com/identity-theft-information/identity-theft-computer-hacking.aspx.

quintessential photo identification."[174] Fraudulent driver's licenses identify, authenticate, and authorize imposters to access services they might not otherwise have. Prior to 9/11, a U.S. driver's license was the only required documentation needed to enter or exit the United States by land into Mexico or Canada.[175] Procedures have been updated to require a passport, but a fraudulent driver's license could be used in a passport application.

This online scheme offers a simple and inexpensive means to acquire a high-quality breeder document without risking exposure at a legitimate license issuing office. Criminal and terrorist organizations can now outsource this skill rather than maintaining internal capability. The identity service provider could be a vital node within criminal and terrorist networks.

2. Illegal Immigration

As of March 2010, the estimated illegal alien population in the United States totaled 11.2 million persons.[176] Specific numbers are not available; however, "it is reasonable to presume that many of these unauthorized aliens are committing document fraud."[177] Employment opportunity draws illegal immigrants into the United States and document fraud offers them the capability to remain undetected. Although federal law prohibits employers from hiring illegal aliens, the employment verification process is fraught with document and identity fraud.[178] While the illegal immigrant population is largely innocuous, the industry they support actively undermines essential identity verification systems. A recent example demonstrates the threat.

---

[174] Gordon et al., "Identity Fraud: A Critical National and Global Threat," 18.

[175] Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, 70.

[176] Jeffrey S. Passel and D'Vera Cohn, "Unauthorized Immigrant Population: National and State Trends, 2010," Pew Hispanic Center (2011), 1.

[177] Ruth Ellen Wassem, "Immigration Fraud: Policies, Investigations, and Issues," Congressional Research Service, RL34007 (2008), 1.

[178] Ibid., 2.

A 44-year-old Pakistani immigrant, Shamsha Laiwalla, established a California business that claimed to handle interactions with the Department of Motor Vehicles (DMV) for paying customers. In addition to her advertized services, she was able to procure valid driver's licenses and breeder documents from California, Nevada, and Washington. An undercover detective, posing as an illegal alien, negotiated with Laiwalla to receive a valid driver's license, "expertly forged" birth certificate and Social Security card with a fraudulent identity in exchange for $3,500.[179]

Laiwalla was part of an extensive network, including DMV employees, which could create valid identification documents and manipulate state records. A joint FBI/LAPD counterterrorism investigation resulted in charges against Laiwalla and 13 accomplices.[180]

This network successfully thwarted all identity issuing security measures by corrupting the license issuing procedure. Once a valid license and breeder documents are obtained, the user has unlimited access to the rights and privileges given to U.S. citizens. Genuine documents that are fraudulently obtained are nearly impossible to trace.

Visa overstays are a part of the immigration process that requires immediate reforms. Immigrants or visitors lawfully enter the United States and then fail to leave when their visas expire. Estimates place current the number of current visa overstays at 4 million to 5.5 million persons.[181] U.S.-VISIT creates a biometric and biographic record for visitors entering the United States, but cannot detect whether visitors leave when expected because no biometric exit data is collected.[182] As a result, entrance and exit data cannot be compared. The *9/11and Terrorist Travel* staff report identified visa

---

179 Joel Rubin, "Counter-terrorism investigators find alleged identity theft ring," *Los Angeles Times*, July 26, 2009, accessed May 26, 2011, http://articles.latimes.com/2009/jul/26/local/me-fraud26.

180 Ibid.

181 U.S. Government Accountability Office, "Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11," GAO-11–919T (Washington, D.C., September 7, 2011): 15.

182 Ibid., 13.

overstays as a common terrorist tactic.[183] If a terrorist were identified after entering into the United States, no mechanism could reliably determine if he or she remained in the country.

Immigrants who enter the United States and overstay their visas must seek employment. Although federal law prohibits employers from hiring illegal aliens, the employment verification process is fraught with document and identity fraud.[184] The E-Verify system offers employers an electronic alternative to paper-based employment verification systems, but a research firm found in 2009 that over 50% of those who were ineligible for employment were found eligible.[185] The U.S. government cannot effectively restrict illegal immigrants from gaining employment because document fraud has significantly undermined its authentication system.

In a 2011 Government Accountability Office (GAO) report, 73% of officers assigned to determine identity for asylum claims reported "it was moderately or very difficult to identify document fraud."[186] This is not surprising, given the availability and relatively low cost of quality identity documents. Incomplete mechanisms for immigrant processing and ineffective immigration enforcement contribute to the undocumented immigrant population. While most are in the United States seeking opportunity, the large undocumented population exponentially complicates efforts to detect terrorists and criminals.

3. Cybercrime

The Internet offers an infrastructure for information sharing that is unparalleled in human history. Users are partially protected by its perceived anonymity and large scale use. However, resourceful cybercriminals have developed tools to target user's private

183 Eldridge et al., *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*, 59.

184 Ruth Ellen Wassem, "Immigration Fraud: Policies, Investigations, and Issues," Congressional Research Service, RL34007 (2008), 1.

185 Ibid., 8

186 U.S. Government Accountability Office, "Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11," GAO-11-919T (Washington, D.C., September 7, 2011): 16.

information. Nefarious programs collectively known as "spyware" are capable of covertly breaching computer security mechanisms, controlling system resources, and/or collecting and distributing personal information.[187]

Hacking allows skilled persons to access personal information from networked systems. Business databases are particularly vulnerable to hacking.[188] In April 2011, 77 million records for a popular gaming console's were hacked.[189] The full extent of the hack could not be determined, however, it was believed that names, addresses, birth dates, e-mail addresses, logins, passwords, and credit card information was compromised.[190] Information of this quality could easily be marketed and sold online. Most companies maintain electronic records and customers are likely to have personal information on file with many different businesses. Customers are completely powerless to prevent this type of theft.

The Internet, in addition to providing an endless source of identity information, can be used in support of other criminal operations. Online credit card schemes offer a source of income and can garnish identity information.[191] Unrestricted international communication supports smuggling operations and movements of money.[192] Transnational terrorists, in particular, have found this capability useful. In 2007, FBI Director Robert Muller testified to Congress that "terrorists increasingly use the Internet to communicate, conduct operational planning, proselytize, recruit, train and to

---

187 Patricia Moloney Figliola, "Spyware: Background and Policy Issues for Congress," Congressional Research Service, RL32706 (2011): 1.

188 Privacy Matters, "Computer Hacking and Identity Theft," accessed March 12, 2012, http://www.privacymatters.com/identity-theft-information/identity-theft-computer-hacking.aspx.

189 Ki Mae Heussner, "Playstation Hack: What You Need to Know," *ABC News*, April 27, 2011, accessed March 12, 2012, from http://abcnews.go.com/Technology/sony-playstation-hack-protect/story?id=13469685.

190 Ibid.

191 Catherine A. Theohary and John Rollins, "Terrorist Use of the Internet: Information Operations in Cyberspace," Congressional Research Service, R41674 (2011): 4.

192 Ibid.

obtain logistical and financial support."[193] Activist hackers, commonly known as "hacktivists," have reportedly provided financial aid to al Qaeda with identity theft and credit card schemes.[194]

Internet fraud schemes, identity theft from spyware, and hacking present uniquely challenging problems for U.S. policymakers. Congress has found it difficult to clearly define the differences between spyware and software designed to enhance the user's experience.[195] Transnational borders complicate efforts to bring offenders to justice. Consequently, Congress has been unable to create meaningful legislation to restrict the use of spyware.[196] Instead, most legislation has been aimed at strengthening information systems and notifying victims after their information has been stolen.[197]

The Internet is a means of identity acquisition, distribution, and fraudulent use. Novices can use it to educate themselves on fraudulent document production or gain access to websites that will generate documents to order.[198] Criminal organizations and terrorists increase their network reach beyond international borders in support of organizational goals. Users demand additional functionality which exposes them to cyber attack, but governments can do little to protect them.

4. Common and Organized Crime

Common criminals, in addition to cybercriminals, erode the foundations of current identity management systems. They utilize stolen identity on a smaller scale than organized crime, but for many of the same reasons. For example, a 2007 U.S. Department of Justice intelligence bulletin reported that methamphetamine users were increasingly using stolen personal checks to purchase items that could be sold or traded

193 Ibid., 5.

194 Catherine A. Theohary and John Rollins, "Terrorist Use of the Internet: Information Operations in Cyberspace," Congressional Research Service, R41674 (2011): 4.

195 Figliola, "Spyware: Background and Policy Issues for Congress," 1.

196 Ibid.

197 Catherine A. Theohary and John Rollins, "Terrorist Use of the Internet: Information Operations in Cyberspace," Congressional Research Service, R41674 (2011): 1.

198 G. R. Gordon et al., "Identity Fraud: A Critical National and Global Threat," 17.

for drugs.[199] Stolen identity information was also used to launder large transfers of money and to make large purchases of cold medication used in the drug manufacturing process.[200]

Criminal record identity theft is an effective tactic used to evade law enforcement. When arrested or cited, an imposter misrepresents himself to law enforcement using stolen identity information.[201] The imposter is then released without repercussion. This tactic also prevents law enforcement from determining if the person they have detained has a prior record or outstanding warrant.[202] Criminal record identity theft complicates law enforcement efforts, allows criminals to walk free, and passes the burden of clearing cases of mistaken identity to victims.[203]

Organized crime takes advantage of networks to bring diverse resources together. Shamsha Laiwalla used her access to clients and connections with corrupt motor vehicles officials to fulfill demand for fraudulent identity documents. Had this network been strategically located across international borders, Laiwalla's arrest would have had a minimal impact. Other actors could quickly fill the vacuum left by her arrest.

Transnational criminal organizations adapt and change dynamically in response to environmental factors. The network structure they use is a function of their adaptive nature. Profit motive is their primary motivation. Strengthening identity systems limits organizational ability to move people and money.

5. Policy Decisions

Policy decisions can have a profound effect on the overall security of identity management systems. Political motivations, poor research data, and/or lobbies influence

---

199 U.S. Department of Justice, "Intelligence Bulletin: Methamphetamine-Related Identity Theft," Product No. 2007-L0424-003 (2007): 2.

200 Ibid.

201 Michael W. Pearl, "It's Not Always about the Money: Why the State Identity Theft Laws Fails to Adequately Address Criminal Record Identity Theft," *The Journal of Criminal Law and Criminology* Vol. 94. No. 1, (2003), 178.

202 Ibid.

203 Ibid., 180.

policymakers to implement changes with consequences that are often beyond the intended effect. For example, New Mexico's driver's license law was intended to create an immigrant-friendly environment but ended up seriously undermining the integrity of the system.

In 2003, New Mexico changed state law to allow immigrants to acquire a driver's license that is exactly the same as that of a U.S. citizen.[204] Applicants are required to provide breeder documents to prove their identity, but cannot be asked about their immigration status. An investigation conducted by the Associated Press discovered serious indications of fraud. Many of the licenses issued had business or fictitious addresses. The investigation found 170 addresses that were listed to 10 or more persons. Some of these could be legitimately explained, but most were attributed to fraud. New Mexico licensing authorities had no mechanism available to detect when multiple licenses were being issued to the same address.

New Mexico's governor, Susana Martinez, cited national security concerns in her attempt to change the law. She surmised that the licenses could "be used to board airplanes, conduct financial transactions, or get another license in some other state."[205] The bill to rescind the law has yet to pass the state Senate and House.

Federal authorities have sought to control state procedures for issuing identity documents through legislation. The REAL ID Act of 2005 is intended to increase security standards and security procedures for the issuing of state driver's licenses. Facilities must upgrade security infrastructure by incorporating cameras, alarms, electronic detection and limiting access to equipment and materials.[206] Information technologies must be interoperable from state-to-state and include software to protect personal information from hackers.[207] Licenses must be tamper-resistant and include

---

204 Barry Massey, "New Mexico's Drivers License Data Point to Fraud," *Fox News*, January 25, 2012, accessed January 26, 2012, from http://www.foxnews.com/us/2012/01/25/ap-enterprise-nm-license-data-points-to-fraud/.

205 Ibid.

206 U.S. Department of Homeland Security, "REAL ID Final Rule," last modified September 14, 2011, http://www.dhs.gov/files/laws/gc_1172765386179.shtm.

207 Ibid.

facial recognition capability.[208] Business practices should be changed have licenses issued from a central processing center to limit employees from corrupting the system.[209] Finally, all breeder documentation provided with an application must be verified.[210]

All 50 states were originally required to be in compliance with the new standards by May 11, 2011, but setbacks forced DHS to push the final compliance date back to January 13, 2013.[211] Many states delayed implementation because of pending legislation, the PASS ID Act of 2009, which would have made these provisions optional.[212] With the final implementation of REAL ID, the United States will have an identity system that is functionally equivalent to a national ID. These measures should significantly increase the validity of genuine state-issued identity tokens. However, the availability of quality fraudulent counterparts threatens to undermine other identity systems.

C. CONCLUSION

The examples above demonstrate some of the many ways that identity systems are undermined resulting in decreased utility. U.S. homeland security depends on systems that can quickly and accurately verify identity persons at ports of entry and deep inside the nation. Underage drinkers, illegal aliens, criminals, poor policy all contribute to weaknesses of the system. The immeasurably large number of fraudulent documents exponentially complicates efforts to detect and apprehend terrorists. Organized crime continues to manufacture documents to meet demand while making a profit and evading law enforcement. These gaps in identity systems have significant detrimental effects on issues that are central to U.S. homeland security.

---

208 Ibid.

209 Ibid.

210 Ibid.

211 U.S. Department of Homeland Security, "REAL ID Final Rule," last modified September 14, 2011, http://www.dhs.gov/files/laws/gc_1172765386179.shtm.

212 Janice Kephart, "The Appearance of Security: REAL ID Final Regulations vs. PASS ID Act of 2009," *Backgrounder* (2009), 1.

Current laws and regulations "tend to deal with the problem in a piecemeal fashion, rather than attacking the big picture."[213] The many complicated aspects of identity management have made comprehensive reform difficult, at best. Weak identity systems have wide ranging effects that cannot be comprehensively understood without the analytical tools used in critical infrastructure. Chapter V will present recommendations for the way ahead using the critical infrastructure framework.

[213] G. R. Gordon et al., "Identity Fraud: A Critical National and Global Threat," 28.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

A. INTRODUCTION

This thesis is focused on providing a thorough understanding of the vulnerabilities associated with weak identity systems and analyzing identity systems as a critical infrastructure. Terrorist travel tactics were explained in order to show security gaps in the international travel system. Organized crime was explored as a potential source of fraudulent documents and compared with terrorism using tools of network analysis. The effects of underage drinkers, illegal immigration, policy decisions, and cyber threats were described to illustrate the range of actors who are actively undermining identity systems.

No single source can determine the net effect that these entities have in degrading identity system utility. However, the critical infrastructure analogy provides a framework necessary to start identifying critical nodes and developing effective strategies to protect system integrity. The structure, function, and widespread use of identity systems necessitate "unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort to bring together government at all levels."[214]

This final chapter will explore the framework of critical infrastructure and draw comparisons with identity systems. Basic principles of security will be discussed to further the analogy and outline recommendations for future policy.

B. CRITICAL INFRASTRUCTURE FRAMEWORK

Critical infrastructure was most recently defined in the USA PATRIOT Act of 2001 as:

> Systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a

[214] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, (2009), accessed May 23, 2011, www.dhs.gov/nipp.

> debilitating effect on security, national economic security, national public health or safety, or any combination of those matters.[215]

The Department of Homeland Security currently recognizes 18 separate sectors of critical infrastructure.[216] Under HSPD-7, the Secretary of DHS was directed to coordinate national efforts to identify, assess, and protect these key assets. This task is infinitely complicated and well beyond the scope of any single bureaucracy. Ted G. Lewis described the challenges of critical infrastructure protection as a "set of wicked problems."[217]

Critical infrastructure is large in terms of geographic size and quantity. The electrical grid, for example, contains an incomprehensible number of miles of power lines. Thousands of electric generating plants feed the system, monitor its load, and respond to electrical demand. Neither the public nor private sectors have direct control of the grid, but regulatory agencies dictate the terms that allow the interconnected plants to operate safely. In reality, the term "grid" is insufficient to describe the electrical system. Electricity is generated and distributed through a system of systems.

The complexity of the electrical system and range of owner/operators makes comprehensive knowledge of intricate nuances of the system nearly impossible.[218] Analytical tools and models are developed to describe and predict system function. This is particularly important when defending system components from attackers such as terrorists. If the most vital components of the system can be identified, then assets can be allocated to protect them.

Network analysis is an important tool used to determine vulnerability.[219] It is used to map and describe the relationship between components, or nodes of a system. A system that can continue to function when multiple critical nodes experience failure is

---

215 42 U.S.C. §5195C(e)

216 U.S. Department of Homeland Security, "Critical Infrastructure," last changed November 30, 2010, http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

217 Lewis, *Critical Infrastructure Protection in Homeland Security,* 49.

218 Ibid., 56.

219 Ibid., 107.

resilient.[220] Conversely, a system that fails when few components are forced offline is brittle.[221] A cascading failure occurs when a small event triggers a series of failures that "propagates throughout a major portion of the infrastructure, ending in calamity."[222] The process of model-based vulnerability analysis (MBVA) allows the system or selected system components to be tested.[223] Once MBVA is conducted, strategies and procedures can be developed to increase system resiliency.

Policymakers conduct risk analysis using MBVA. [224] Analyzing risk is a process of making decisions to allocate resources to protect critical nodes and maximize system utility. Budgetary constraints limit the amount of resources available to harden critical nodes.[225] System function, nature of the threat, and intended result will shape how these resources are spent. Given that disruptions can be caused by nature or man, responses should be developed from an "all-hazards" approach.[226] This approach mitigates system disruption by tailoring responses to meet the most-likely threats. A chemical spill, for example, could be caused by an accidental train derailment or intentional terrorist act. Regardless of the cause, first-responders must have equipment and trained personnel available to counter the threat.

Ted G. Lewis identified the seven major challenges to infrastructure protection as vastness, control, information sharing, interdependencies, system knowledge, inadequate analytical tools, and asymmetric conflict.[227] Each of these challenges translates seamlessly to identity systems.

Identity management is facilitated by vast a system of systems. Interconnected databases, under public and private control, support a multitude of transactions.

---

220 Schneier, *Beyond Fear*, 120.

221 Ibid.

222 Lewis, *Critical Infrastructure Protection in Homeland Security*, 96.

223 Ibid., 107.

224 Ibid., 147.

225 Ibid.

226 U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, (2009), accessed May 23, 2011, www.dhs.gov/nipp.

227 Ibid., 49–50.

Customers and service providers depend on identity systems to return immediate and accurate results when queried. Roles, responsibilities, and system function are simplistic at a large scale. However, complexity of the system and of these relationships rises exponentially as scale decreases.

Decreasing the scale of identity systems brings this narrative to uncharted territory. This thesis has argued that identity is a system and asset, physical and virtual, vital to the United States that would have a debilitating effect on national and economic security if incapacitated. Acceptance of this description would necessitate observing identity management systems as a stand-alone sector of critical infrastructure.

Current analytical tools of identity systems, as a sector, are virtually nonexistent. Statistical data and policy analysis indicates significant system degradation. Network analysis is needed to model major components of the overall system so that vulnerabilities can be clearly identified and resources effectively managed. Formal observation of this sector would allow federal funding to be allocated and would assign federal agencies to develop a sector-specific plan.

U.S. national security depends on stronger identity systems. Passports and driver's licenses are important token identifiers that have been significantly undermined by theft and fraud. Securing these systems from terrorists and criminal organizations would constitute an all-hazards approach to national security. Recommendations for increasing security must take into account the basic functions of all identity systems.

C. IDENTIFY, AUTHENTICATE, AUTHORIZE[228]

Identity systems, as a meta-sector or stand-alone sector of critical infrastructure, are expected to perform three basic functions. They should identify, authenticate, and authorize. Figure 4 depicts the interaction of these functions.

228 Schneier, *Beyond Fear*, 120.

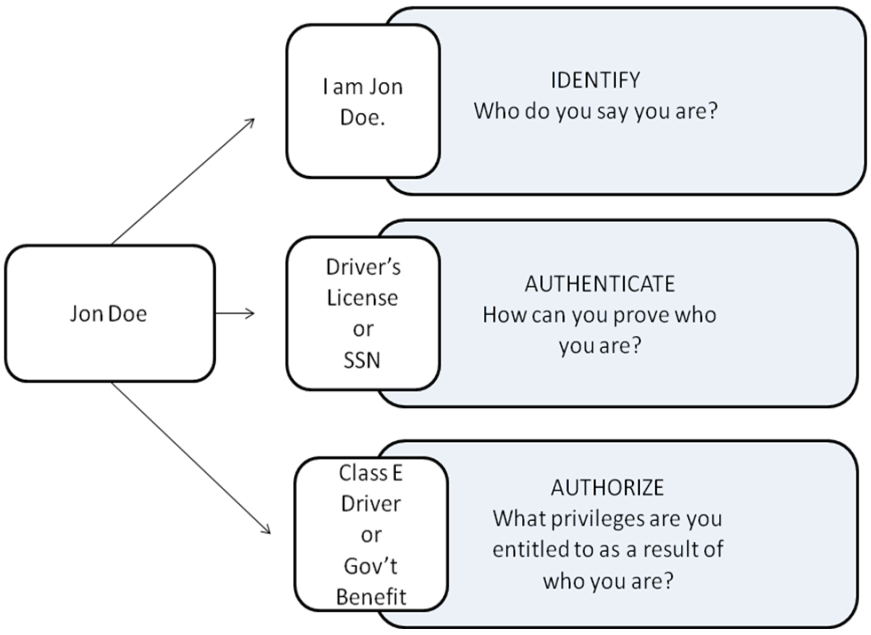

Figure 4. Identify, Authenticate, and Authorize Diagram

The first step in any identity system is *identification* or "the act [or process] of recognizing or establishing as being a particular person."[229] In small groups, individuals are distinguished visually or by name.[230] In larger complex systems, transactions must take place between persons who have never met. A name and account number, or similar combination of specific identifiers helps prevent misidentification between persons with the same name. Transactions in identity systems begin when a person expresses, "This is who I am, and this is what I want."

Authentication is the second process whereby identity is verified. This can be accomplished by something a person knows (knowledge-based), something he has (token-based), or something he is (biometric).[231] Knowledge-based identifiers are passwords or information that should be unique to the presented identity. Pharmacists always ask for name and birth date when customers pick up prescriptions. Chances are

229 Clarke, "Human Identification in Information Systems: Management Challenge and Public Policy Issues," 7.

230 Schneier, *Beyond Fear,* 186.

231 Ibid.

good that only one person with that particular combination of name and birth date will conduct business at that store. However, there is always a possibility that another person could have the same combination or misrepresent themselves if they know the combination of identity and knowledge-based authentication of another person.

Authentication is token-based when identity cards or physical items that confirm identity are used. Driver's licenses and passports are common token identifiers. They contain information that can be verified to facilitate a particular transaction. In order to purchase alcohol, a person must be able to prove he is over the age of 21. A driver's license is commonly used for this purpose. Major portions of this thesis have shown that token-based identifiers are susceptible to manipulation or counterfeiting.

Modern technology has increased the accuracy and specificity of the authentication process using biometrics. Fingerprints, iris scanning, and facial recognition software offer an accurate authentication rate well in excess of 90%. Unique physical identifiers are scanned, stored in a database, and then compared against subsequent scans. The U.S.-VISIT system uses fingerprint technology for this purpose. However, the system can be undermined if a person successfully misrepresents his identity to authorities and his biometric data is associated with a fraudulent identity.

The third function of identity systems is *authorization*. After a person has been identified and authenticated, authorization determines the rights or privileges he is entitled to. A driver's license is a token that supports identity and authorizes that the bearer has the privilege to drive a motor vehicle. A passport supports identity and authorizes the bearer to all rights and privileges bestowed to a citizen of its issuing nation. Terrorists steal passports in order to create fraudulent tokens that misrepresent their true identity and grant authorizations such as access to target countries.

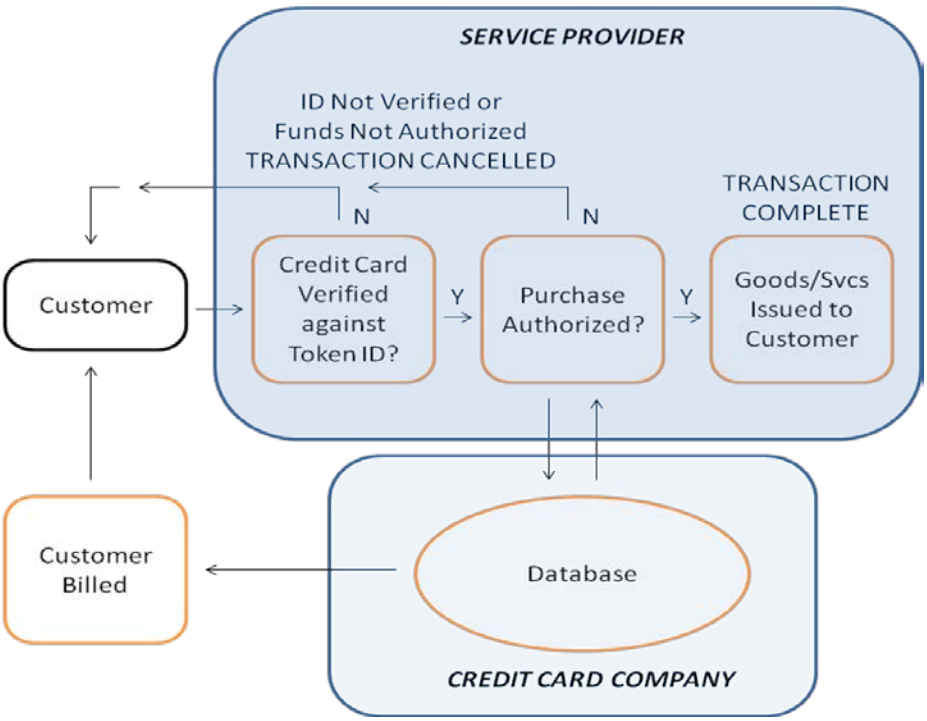

Figure 5. Prototypical Credit Card Transaction

Figure 5 diagrams a prototypical credit card transaction. The customer *identifies* himself to a service provider and presents a credit card for payment. The service provider *authenticates* the customer's identity by checking the credit card against a picture ID. Correlation between the imprinted name on the credit card and photo ID is usually sufficient for most transactions. The credit card company's database is queried, funds are *authorized*, and the purchase is complete. The customer is subsequently billed for all purchases made throughout the month.

This description represents an ideal scenario. Most service providers choose to bypass authenticating credit cards against a photo ID because this step inconveniences the customer. They presume that the majority of transactions are legitimate and accept risk by not checking authenticating all payments. Profit motives dictate that the speed of the transaction is more important than accuracy. Losses are estimated and factored into costs. Systems that do not identify, authenticate, and authorize, are susceptible to fraud.

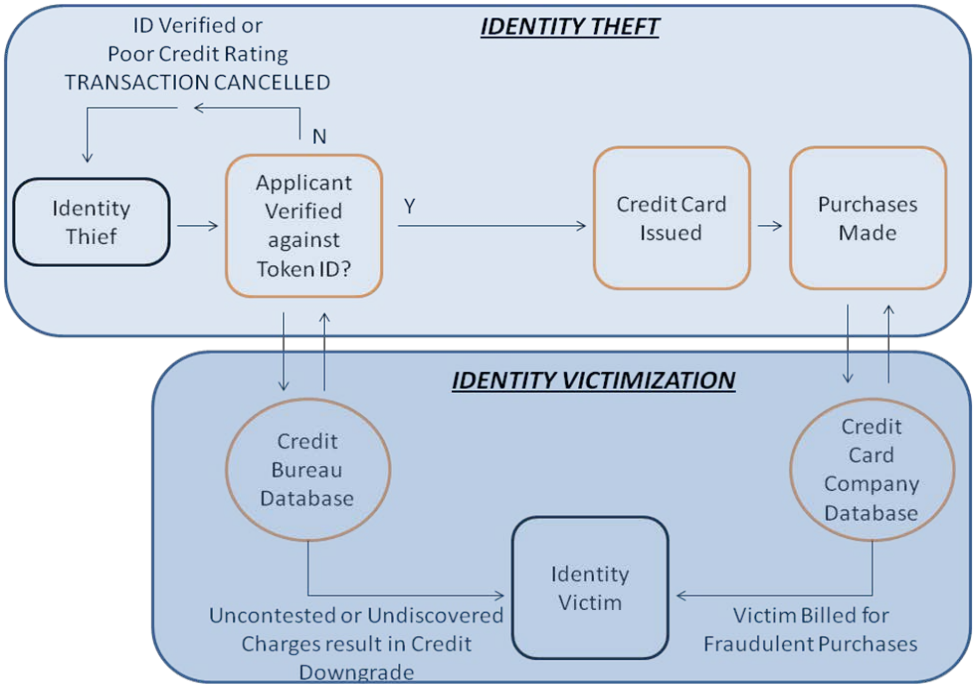

Figure 6. Identity Theft and Victimization

Identity theft occurs when an imposter successfully hacks one or more components of an identity system. Figure 6 describes the fraudulent acquisition of credit using stolen information. An imposter identifies himself as using a victim's information. Credit is issued in the victim's name after the lending company fails to properly authenticate the imposter applicant. Purchases accumulate and the victim is billed. If the victim's address is not used on the credit application, the account could be sent to collections and reported to the credit bureaus without the victim ever knowing.

This scenario is repeated thousands of times per year. Once a victim is aware his information is compromised, he is essentially powerless to prevent it from being used. The credit bureaus offer a 90 day credit alert that should flag the account and require a lender to contact the account holder before issuing credit. But this action is voluntary and the lenders would rather assume risk than inhibit a transaction.

These scenarios show the importance of interlacing processes in identity networks. Authentication is time consuming and difficult. Service providers choose to assume risk in order to increase the volume of transactions and decrease customer

inconvenience. This level of risk is unacceptable in the international travel system. Homeland security enterprises require resilient identity systems that are effective and efficient.

Identity systems should be analyzed as a critical infrastructure. The process to identify, authenticate, and authorize is a sector-specific framework that is used to locate faults and provide greater resolution of system function. This framework enhances existing critical infrastructure terminology and increases its relevance to identity systems.

D. RECOMMENDATIONS FOR THE WAY AHEAD

Identity systems are hacked when persons misrepresent themselves and receive authorizations that they are not entitled to. All three functions of identity systems must work in concert to protect the integrity of the system. Layering identity techniques and systems decreases the chances for failure and increases resiliency. This thesis demonstrates that many identity systems do not meet these criteria.

Passport issuance, for example, is lacking an authentication mechanism. DoS officials have accepted fraudulent token identifiers (i.e., birth certificates, driver's licenses) and issued passports because of bureaucratic and technical limitations on information sharing.[232] Both barriers can be theoretically breached, but would require significant financial and political support. Formalizing identity systems as a critical infrastructure sector is an important step towards this goal. Standardizing identity issuing and verification procedures is needed to increase reliability of authentication tokens.

The REAL ID act of 2005 requires states to meet minimum standards for issuing driver's licenses and ID cards. Applicants must present multiple breeder documents that must all be verified. Security infrastructure must be in place to deter issuing authorities from corrupt behavior. Databases must be interoperable from state-to-state to facilitate data verification. All information systems must be protected with encryption software to prevent hackers from gaining access to personal records. REAL ID standards should be

[232] GAO, "Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process," GAO-09-447 (Washington, D.C., March 2009): 10.

comprehensively and universally implemented. States that refuse to comply or reallocate DHS funding should be punitively punished by withholding federal funds. Homeland security is contingent upon secure ID issuing procedures.

Increasing interoperability by connecting state information databases is an important component of REAL ID, but one that creates a new threat. State employees would suddenly have access to significantly more information than ever before. Increasing system utility also makes the system a more appealing target for thieves. Access to an interstate database should be restricted to as few persons as possible. These trusted few should be subject to an extensive background and credit check, similar to those seeking a security clearance in the U.S. military. Information compartmentalization and two-person integrity are effective methods for ensuring database access is not misused.

REAL ID standards significantly increase the reliability of genuine authentication tokens. However, quality fraudulent documents are widely available from multiple sources. No single authentication token should be accepted as proof of identity for most transactions. Relying on a single token for authentication constitutes a brittle system. Verification mechanisms must be built into the system to check identity tokens against databases. For instance, airport security personnel should have the capability to swipe any driver's license and instantly have the accompanying state record displayed. This type of system dramatically decreases the utility of a fraudulent ID token since security personnel can immediately compare the traveler's appearance with the token picture, and picture on file. Restricting system access by removing active search capability prevents records from arbitrary searches, preventing misuse.

Government-maintained identity databases carry particular importance because of the authorizations they provide, but businesses maintain the vast majority of personal information. The average consumer has no insight as to the quality of identity system management with a company. The Federal Trade Commission should develop a voluntary annual certification process for participating businesses. A scalar system would give consumers ratings to compare before divulging personal information. Conversely, businesses would have incentive to acquire a certification and the highest

possible rating. This system would take advantage of market competition to strengthen information systems and overall economic security.

E. CONCLUSION

Identity management systems meet the prima facie elements for critical infrastructure. Protection of these systems is essential to homeland and economic security. A layered approach to security is essential to strengthen the functions of the system. Policy options to strengthen systems need to be effective and efficient. Analyzing identity management systems as a critical infrastructure provides the framework necessary to make informed policy decisions.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Anderson, Keith B. "Who are the Victims of Identity Theft? The Effect of Demographics." *Journal of Public Policy & Marketing* 25, no. 2 (2006): 160–171.3

Arquilla, John, and David Ronfeldt. *Networks and Netwar: The Future of Terror, Crime, and Military.* Santa Monica, CA: RAND, 2001.

Avila, Jim. "Risky Business: Teens Buying Fake IDs From Overseas Via Internet." *ABC News.* August 5, 2011. http://abcnews.go.com/U.S./ParentingWeek/risky-business-teens-buying-fake-ids-overseas-Internet/story?id=14243205#.TkVKVfdgn4M.e-mail (accessed August 15, 2011).

Chen, Hsinchun. "Exploring Extremism and Terrorism on the Web: The Dark Web Project." In *PAISI '07 Proceedings of the 2007 Pacific Asia Conference on Intelligence and Security Infomatics*, edited by Christopher C. Yang, 1–20. Heidelburg: Springer-Verlag Berlin, 2007.

Chiu, Chaochang, Yungchang Ku, Ting Lie, and Yuchi Chen. "Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches." *International Journal of Electronic Commerce* 15, no. 3 (2011): 123–147.

Clarke, Roger. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." *Information Technology & People* 7, no. 4 (2004): 6–37.

Collins, Judith M. *Investigating Identity Theft: A Guide for Businesses, Law Enforcement, and Victims.* Hoboken, NJ: John Wiley & Sons, Inc, 2006.

Federal Trade Commission. "Take Charge: Fighting Back Against Identity Theft." February 2003. http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf (accessed June 1, 2011).

Figliola, Patricia Moloney. "Spyware: Background and Policy Issues for Congress." Congressional Research Service RL32706 (January 2011): 1–7.

"Filling Out Arrival-Departure Record, CBP Form I-94, for Nonimmigrant Visitors with a Visa for the U.S." *U.S. Department of Homeland Security.* July 2, 2010. http://www.cbp.gov/xp/cgov/travel/id_visa/i-94_instructions/filling_out_i94.xml (accessed Mar 10, 2012).

Finklea, Kristin M. "Identity Theft: Trends and Issues." *Congressional Research Service* R40599 (2010): 1–27.

———.“Identity Theft: Trends and Issues.” Congressional Research Service R40599 (2012): 1–28.

Gordon, Gary R., Jr., Norman A. Wilcox, Donald J. Rebovich, Thomas M. Regan, and Judith B. Gordon. “Identity Fraud: A Critical National and Global Threat.” *Journal of Economic Crime Management* 2, no. 1 (October 2004): 1–48.

Halperin, Ruth, and James Backhouse. “A Roadmap for Research in Identity Theft in the Information Society.” *Identity Journal Limited* 1, no. 1 (December 2008): 71–87.

Hamill, J. Todd, Richard F. Deckro, W. James Chrissis, and Robert F. Mills. “Analysis of Layered Social Networks.” *IO Sphere*, 2008: 27–33.

Harty, Nancy. “Fake IDs Made in China Seized; Underage Kids Cited.” *CBS News.* July 22, 2011. http://chicago.cbslocal.com/2011/07/22/fake-ids-made-in-china-seized-underage-kids-cited/#.TkVH-8IFfV4.e-mail (accessed August 15, 2011).

Heussner, Ki Mae. “Playstation Hack: What You Need to Know.” *ABC News.* April 27, 2011. http://abcnews.go.com/Technology/sony-playstation-hack-protect/story?id=13469685 (accessed March 12, 2012).

Kean, Thomas H., et al. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* Washington D.C.: National Commission on Terrorist Attacks upon the United States, 2004.

Kephart, Janice. “The Appearance of Security: REAL ID Final Regulations vs. PASS ID Act of 2009.” *Backgrounder*, 2009.

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Hoboken, NJ: John Wiley & Sons, 2006.

LoPucki, Lynn. “Human Identification and the Identity Problem.” *Texas Law Review* 80 (2001): 89–137.

Makarenko, Tamara. “The Crime-Terror Continuum: Tracing the Interplay between Transnational Organized Crime and Terrorism.” *Global Crime* 6, no. 1 (February 2004): 129–145.

Massey, Barry. “New Mexico’s Drivers License Data Point to Fraud.” *Fox News.* January 25, 2012. http://www.foxnews.com/us/2012/01/25/ap-enterprise-nm-license-data-points-to-fraud/. (accessed January 26, 2012).

Mew, Barry G. “From Pakistan to the United States: U.S. Postal Inspectors Untane a Web of Mail Fraud, Credit Card Fraud, Internet Fraud, and Identity Theft.” *United States Postal Inspection Service Bulletin* 51, no. 1 (2003): 36–38.

Office of Travel and Tourism Industries. “International Visitation to the United States: A Statistical Summary of U.S. Visitation.” *U.S. Department of Commerce.* 2010. http://tinet.ita.doc.gov/outreachpages/download_data_table/2010_Visitation_Report.pdf (accessed March 10, 2012).

Olson, L. Eric, A. David Shirk, and Andrew Selee, . *Shared Responsibility: U.S.-Mexico Policy Options for Confronting Organized Crime.* Washington D.C.: Woodrow Wilson International Center for Scholars, 2010.

Passel, Jeffery S., and D’Vera Cohn. “Unauthorized Immigrant Population: National and State Trends.” *Pew Hispanic Center.* February 1, 2011. http://www.pewhispanic.org/files/reports/133.pdf (accessed March 2, 2012).

Pearl, Michael W. “It’s Not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft.” *The Journal of Criminal Law & Criminology* Vol. 94, no. 1 (November 2003): 169–208.

Perri, Frank S., and Richard G. Brody. “The Dark Triad: Organized Crime, Terror and Fraud.” *Journal of Money Laundering Control* 14, no. 1 (2011): 44–59.

Picarelli, John T., and Louise I. Shelley. “Organized Crime and Terrorism.” In *Terrorism Financing and State Responses*, edited by Jeanne K. Giraldo and Harold A. Trinkunas. Stanford: Stanford University Press, 2007.

Privacy Matters. *Computer Hacking and Identity Theft.* http://www.privacymatters.com/identity-theft-information/identity-theft-computer-hacking.aspx (accessed March 2012, 2012).

Raab, Charles D. *Social and Political Dimensions of Identity.* Vol. 262, in *The Future of Identity in the Information Society*, by Charles D. Raab, 3–19. Boston: Springer, 2009.

Rubin, Joel. “Counter-Terrorism investigators find alleged identity theft ring.” *Los Angeles Times.* July 26, 2009. http://articles.latimes.com/2009/jul/26/local/me-fraud26 (accessed June 1, 2011).

Rudner, Martin. “Misuse of Passports: Identity Fraud, the Propensity to Travel, and International Terrorism.” *Studies in Conflict & Terrorism* 31 (2008): 95–110.

Schmidt, Howard A. “National Strategy for Trusted Identities in Cyberspace.” *The White House.* April 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (accessed June 1, 2011).

Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in and Uncertain World.* New York: Copernicus Books, 2003.

Schwartz, Carly. "Olajide Oluwaseum Noibi Sentenced to Time Served in LA Stowaway Case." *Huffington Post.* November 28, 2011. http://www.huffingtonpost.com/2011/11/28/olajide-oluwaseun-noibi-stowaway_n_1117716.html (accessed January 16, 2012).

Seghetti, Lisa M., and Stephen R. Vina. "U.S. Visitor and immigrant Status Indicator Technology (U.S.-VISIT) Program." Congressional Research Service RL32234 (2005): 1–36.

The White House. "Homeland Security Presidential Directive / HSPD-7." *Federation of American Scientists.* December 17, 2003. http://www.fas.org/irp/offdocs/nspd/hspd-7.html (accessed June 1, 2011).

Theohary, A. Catherine, and John Rollins. "Terrorist Use of the Internet: Information Operations in Cyberspace." Congressional Research Service R41674 (2011): 1–26.

U.S. Department of Homeland Security. "Critical Infrastructure." November 30, 2010. http://www.dhs.gov/files/programs/gc_1189168948944.shtm (accessed March 03, 2012).

———. "Biometric Standards Requirements for U.S.-VISIT." March 15, 2010. http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_biometric_standards.pdf (accessed March 9, 2012).

———. "Government Agencies Using U.S.-VISIT." March 2011, 2011. http://www.dhs.gov/files/programs/gc_1214422497220.shtm (accessed March 6, 2012).

———. "National Infrastructure Protection Plan." 2003. www.dhs.gov/nipp (accessed May 23, 2011).

———. "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland." February 2010. http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (accessed June 1, 2011).

———. *REAL ID Final Rule.* September 14, 2011. http://www.dhs.gov/files/laws/gc_1172765386179.shtm (accessed March 2, 2012).

U.S. Department of Justice. “A National Strategy to Combat Identity Theft.” *Office of Community Oriented Policing Services.* 2006. http://www.cops.usdoj.gov/files/ric/Publications/e03062303.pdf (accessed June 1, 2011).

———. “Intelligence Bulletin: Methamphetamine-Related Identity Theft.” Product No. 2007-L0424–003 (2007): 1–4.

———. “Strategic Plan: Stewards of the American Dream.” *Department of Justice.* 2007–2012. http://www.justice.gov/jmd/mps/strategic2007–2012/strategic_plan20072012.pdf (accessed June 1, 2011).

U.S. Government Accountability Office. “Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers.” GAO-11–674T (May 2011).

———. “Combating Terrorism: Additional Steps Needed to Enhance Foreign Partner’s Capacity to Prevent Terrorist Travel.” GAO-11–667 (July 2011): 1–42.

———. “Counterfeit Identification and Identity Fraud raise Security Concerns.” GAO-03–1147T (May 2011).

———. “Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11.” GAO-11–919T (September 2011): 1–31.

———. “Department of State: Undercover Tests Reveal Significant Vulnerabilities in State’s Passport Issuance Process.” GAO-09–447 (March 2009): 1–14.

———. “Homeland Security: Key U.S.-VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed.” GAO-10–13 (November 2009): 1–52.

U.S. Immigration and Customs Enforcement. “ICE Strategic Plan.” 2010–2014. http://www.ice.gov/doclib/news/library/reports/strategic-plan/strategic-plan-2010.pdf (accessed June 1, 2011).

U.S. Transportation Security Administration. “Secure Flight Program.” http://www.tsa.gov/what_we_do/layers/secureflight/ (accessed March 10, 2012).

Wassem, Ruth Ellen. “Immigration Fraud: Policies, Investigations, and Issues.” Congressional Research Service RL34007 (April 2008): 1–18.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California